Graduate Texts in Mathematics

Jean-Pierre Escofier

Galois Theory

Springer

Graduate Texts in Mathematics 204

Springer Science+Business Media, LLC

Graduate Texts in Mathematics

(continued after index)

Jean-Pierre Escofier

Galois Theory

Translated by Leila Schneps

With 48 Illustrations

Springer

Jean-Pierre Escofier
Institute Mathematiques de Rennes
Campus de Beaulieu
Université de Rennes 1
35042 Rennes Cedex
France
jean-pierre.escofier@univ-rennesl.fr

Translator
Leila Schneps
36 rue de l'Orillon
75011 Paris
France
leila.schneps@ens.fr

Mathematics Subject Classification (2000): 11R32, 11S20, 12F10, 13B05

Library of Congress Cataloging-in-Publication Data
Escofier, Jean-Pierre.
Galois theory / Jean-Pierre Escofier.
p. cm. — (Graduate texts in mathematics; 204)
Includes bibliographical references and index.
ISBN 978-1-4612-6558-0 ISBN 978-1-4613-0191-2 (eBook)
DOI 10.1007/978-1-4613-0191-2
1. Galois theory. I. Title. II. Series.
QA174.2 .E73 2000
512'.3—dc21 00-041906

Printed on acid-free paper.

Translated from the French *Théorie de Galois*, by Jean-Pierre Escofier, first edition published by Masson, Paris, © 1997, and second edition published by Dunod, Paris, © 2000, 5, rue Laromiguière, 75005 Paris, France.

Production managed by Francine McNeill; manufacturing supervised by Joe Quatela.
Photocomposed copy prepared from the translator's TeX files.

9 8 7 6 5 4 3 2 1

ISBN 978-1-4612-6558-0 SPIN 10711904

Preface

This book begins with a sketch, in Chapters 1 and 2, of the study of algebraic equations in ancient times (before the year 1600). After introducing symmetric polynomials in Chapter 3, we consider algebraic extensions of finite degree contained in the field $\mathbb{C}$ of complex numbers (to remain within a familiar framework) and develop the Galois theory for these fields in Chapters 4 to 8. The fundamental theorem of Galois theory, that is, the Galois correspondence between groups and field extensions, is contained in Chapter 8. In order to give a rounded aspect to this basic introduction of Galois theory, we also provide

- a digression on constructions with ruler and compass (Chapter 5),
- beautiful applications (Chapters 9 and 10), and
- a criterion for solvability of equations by radicals (Chapters 11 and 12).

Many of the results presented here generalize easily to arbitrary fields (at least in characteristic 0), or they can be adapted to extensions of infinite degree.

I could not write a book on Galois theory without some mention of the exceptional life of Évariste Galois (Chapter 13). The bibliography provides details on where to obtain further information about his life, as well as information on the moving story of Niels Abel.

After these chapters, we introduce finite fields (Chapter 14) and separable extensions (Chapter 15). Chapter 16 presents two topics of current research:

firstly, the inverse Galois problem, which asks whether all finite groups occur as Galois groups of finite extensions of $\mathbb{Q}$ and which we treat explicitly in one very simple case, and secondly, a method for computing Galois groups that can be programmed on a computer.

Most of the chapters contain exercises and problems. Some of the statements are for practice, or are taken from past examinations; others suggest interesting results beyond the scope of the text. Some solutions are given completely, others are sketchy, and certain solutions that would involve mathematics beyond the scope of the text are omitted completely.

Finally, this book contains a brief sketch of the history of Galois theory. I would like to thank the municipal library in Rennes for having allowed me to reproduce some fragments of its numerous treasures.

The entire book was written with its student readers in mind, and with constant, careful consideration of the question of what these students will remember of it several years from now.

I owe tremendous thanks to Annette Houdebine-Paugam, who helped me many times, and to Bernard Le Stum and Masson, who read the later versions of the text and suggested many corrections and alterations.

Jean-Pierre Escofier
May 1997

Contents

1

Historical Aspects of the Resolution of Algebraic Equations

In this chapter, we briefly recall the many different aspects of the study of algebraic equations, and give a few of the main features of each aspect. One must always remember that notions and techniques which we take for granted often cost mathematicians of past centuries great efforts; to feel this, one must try to imagine oneself possessing only the knowledge and methods which they had at their disposal. The bibliography contains references to some very important ancient texts as well as some recent texts on the history of these subjects (see, in particular, the books by J.-P. Tignol and H. Edwards and the articles by C. Houzel).

1.1 Approximating the Roots of an Equation

Around the year 1600 B.C., the Babylonians are known to have been able to give extremely precise approximate values for square roots. For instance, they computed a value approximating $\sqrt{2}$ with an error of just 10^{-6}. In sexagesimal notation, this number is written 1.24.51.10, which means

$$1 + \frac{24}{60} + \frac{51}{60^2} + \frac{10}{60^3} = 1,41421296\ldots.$$

Later (around the year 200 A.D.), Heron of Alexandria sketched the well-known method of approximating square roots by using the sequence

$$u_{n+1} = \frac{1}{2}\left(u_n + \frac{a}{u_n}\right).$$

It is not possible to give here the full history of approximations as developed by Chinese (who computed cube roots as far back as 50 B.C.) and Arab mathematicians. Note, however, that the linearization method developed by Isaac Newton using the sequence

$$u_{n+1} = u_n - \frac{f(u_n)}{f'(u_n)}$$

was already known to the Arab mathematician Sharaf ad Din at Tusi, born in 1201.

In 1225, Leonard of Pisa gave the approximate value 1.22.7.42.33.40 (in base 60) for the positive root of the equation $x^3 + 2x^2 + 10x = 20$. It is an excellent approximation, with an error on the order of just 10^{-10}; we do not know how he obtained it.

1.2 Construction of Solutions by Intersections of Curves

The Greeks were able to geometrically construct every positive solution of a quadratic equation, using intersections of lines and circles, but they did not formulate this problem in an algebraic manner. We will return to their procedures in Chapter 5. To solve cubic equations, they used conics, as did Omar Khayyam around 1100 (see §2.2.2); perhaps this method was already understood by Archimedes (287–212 B.C.).

In his book *Geometry*, one of three treatises attached to his grand work *Discours de la Méthode*, René Descartes related solutions of algebraic equations to intersections of algebraic curves. This theme is one of the sources of algebraic geometry.

1.3 Relations with Trigonometry

The division of the circle into a certain number of equal parts, or *cyclotomy* (coming from a Greek word), was the object of a great deal of study. By studying the construction of the regular nine-sided polygon, which leads to a cubic equation, mathematicians of the Arab world revealed the relation, subsequently described also by François Viète (1540–1603), between the trisection of an angle and the solution of a cubic equation (see Exercise 2.5). Viète also gave formulas expressing $\sin n\theta$ and $\cos n\theta$ as functions of $\sin\theta$ and $\cos\theta$. Laurent Wantzel showed in 1837 that the problem posed by the Greeks, of trisecting an arbitrary angle using only a ruler and a compass, was impossible (see §5.6).

Probably inspired by work of Alexandre Vandermonde dating back to 1770, Carl Friedrich Gauss showed how to given an algebraic solution for

the division of the circle into p equal parts whenever p is a Fermat prime ($p = 17, 257, 65537$); his results are presented in the seventh part of his *Disquisitiones arithmeticae* published in 1801, which prepared the way for Abel and Galois.

1.4 Problems of Notation and Terminology

Before the 17th century, mathematicians usually did not use any particular notation; it is easy to conceive of the difficulty of developing algebraic methods under these conditions! Modern notation was more or less developed by Descartes, who used it in his book *Geometry.*

Let us give an idea of the notation used by Viète. In his *Zététiques* (1591, from the Greek $\zeta\eta\tau\varepsilon\iota\nu$, meaning "search"), the expression

$$\frac{F \cdot H + F \cdot B}{D + F} = E$$

is written

$$\left\{\begin{array}{ccc} F & \text{in} & H \\ +F & \text{in} & B \\ \hline D & + & F \end{array}\right\} \quad \text{æquabitur } E.$$

Viète's notation for powers of the unknown is very heavy: he writes "A quadratum" for A^2, "A cubus" for A^3, "A quadrato-quadratum" for A^4, etc., and "A potestas," "A gradum" for A^m, A^n. To indicate the dimension of the parameter F, he writes "F planum" for F of dimension 2, "F solidum" for F of dimension 3, etc.

For example, for the general equation of the second degree in A, Viète, who always assumes homogeneity of dimension between the variables and the parameters B, D, Z, writes:

$$B \text{ in A quadratum plus D plano in A æquari Z solido,}$$

i.e. $BA^2 + DA = Z.$

This condition of homogeneity was definitively abandoned only around the time of Descartes (see §5.7). The great contribution of Viète was the creation of a system of computation with letters used to represent known or unknown quantities (*logistice speciosa*, as opposed to *logistice numerosa*). This idea produced a deep transformation in the methods and conception of algebra; instead of working only on numerical examples, one could consider the general case. The economy of thought produced by this approach, and the new understanding it gave rise to, made further progress possible. Certainly, letters had been used before Viète, but not in actual computations; one letter would be used for a certain quantity, another for its square, and so forth.

Viète was known in his time as a counselor of Henri III, and that he was a counselor in the Parliament of Bretagne in Rennes from 1573 to 1580.

Let us give some of the main turning points in the history of algebraic notation.

Decimals were introduced by Al Uqlidisi, the *Euclidean* (around 950), as well as by Al Kashi (1427), Viète (1579), Simon Stevin (1585). The use of a point to separate the integer and fractional parts of a number was made popular by John Neper (in France, a comma is used instead of a point). But even long after the introduction of the point, people continued to write a number as an integer followed by its fractional part in the form of a fraction: $11\frac{224\,176}{1\,000\,000}$.

The signs + and − were already in use around 1480 (+ was apparently a deformation of the symbol &), but by the beginning of the 17th century, they were used generally. Multiplication was written as M by Michael Stifel (1545), and as *in* by Viète (1591); our current notation dates back to William Oughtred (1637) for the symbol ×, and to Wilhelm Leibniz (1698) for the dot.

For powers of the unknown, $1,225 + 148\ x^2$ was written as $1,225\,\tilde{p}\,148^2$ by Nicolas Chuquet (1484), $3x^2$ was written as $3\overset{2}{\smile}$ by Raffaele Bombelli (1572), whereas Stevin wrote 3③+ 5②− 4① for $3x^3 + 5x^2 - 4x$. The exponential notation x^2, x^3, etc., came with Descartes, whose formulas are actually written in a notation very close to our own. In the 18th century, one sees bb for b^2, but b^3, b^4, etc.

Only after methods of explicit computation and exponential notation had been perfected did it become possible to think clearly about computing with polynomials. Descartes showed that a polynomial vanished at the value a if and only if it was divisible by $X - a$. The history of the manner of referring to the unknown is extremely complicated, and we will not describe it here. The symbol = used by Michel Recorde (1557) came to replace the symbol used by Descartes, an α written backward, toward the end of the 17th century, thanks to Leibniz. Albert Girard (1595–1632) introduced the notation $\sqrt[3]{\ }$, which he substituted for ($\frac{1}{3}$); he also introduced the abbreviations for sine and tangent, and used the symbols $<$, $>$ like Harriot. Indices were introduced by Gabriel Cramer (1750) to write his famous formulas (the use of primes $'$, $''$, $'''$ followed by ^{iv}, ^{v} etc. became widespread around the same time); indices of indices were introduced by Galois. The symbol $\sum$ was introduced by Leonhard Euler (1707–1783). These notations passed into general usage only during the 20th century.

1.5 The Problem of Localization of the Roots

This problem concerns polynomials with real coefficients. The results of Descartes based on the number of sign changes in the sequence of coeffi-

cients (see Exercise 3.7) were perfected in the 19th century by Jean-Baptiste Fourier and François Budan, and then by Charles Sturm, who in 1830 gave an algorithm to determine the number of real roots in a given interval.

1.6 The Problem of the Existence of Roots

Al Khwarizmi appears to have been the first, around the year 830, to have pointed out the existence of quadratic equations having two strictly positive roots (see, however, §2.1.1). Negative roots were taken into consideration only around the end of the 16th century (see §2.1.4).

Girard was the first to assert that an equation of degree (or *denomination*, as he said) n has n roots (Figure 1.1). He did not give any proof and his ideas about the exact nature of the solutions seem rather vague; he thought of them as complex numbers *or other similar numbers.* This vagueness did not prevent him from innovating the use of computations with roots as though they were numbers (see §3.4). Every mathematician will appreciate his wonderful formulation

"pour la certitude de la reigle generale"

(for the certitude of the general rule).

II. Theoreme.

Toutes les equations d'algebre recoivent autant de ſolutions, que la denomination de la plus haute quantité le demonſtre, excepté les incomplettes

Explication.

Soit une equation complette 1 (4) eſgale 4 (3) + 7 (2) — 34 (1) — 24 : alors le denominateur de la plus haute quantité eſt (4), qui ſignifie qu'il y a quatre certaines ſolutions, & non plus ny moins, comme 1, 2, — 3, 4

Donc il ſe faut reſouvenir d'obſerver tousjours cela : on pourroit dire à quoy ſert ces ſolutions qui ſont impoſſibles, je reſpond pour trois choſes, pour la certitude de la reigle generale, & qu'il ny a point d'autre ſolutions, & pour ſon utilité

FIGURE 1.1. Excerpt from Girard's *Invention nouvelle en l'algèbre...*, 1629

Descartes was less precise about the number of roots, simply bounding it by the degree of the equation: "Autant que la quantité inconnue a de dimensions, autant *peut-il* y avoir de diverses racines." ("As many as the dimensions of the unknown quantity, as many there *may be* different roots.") The nature of the roots also escaped Leibniz, who did not see that $\sqrt{\sqrt{-1}}$ is a complex number (1702). But the methods of integration of rational functions, which were developed by Leibniz and Jean Bernoulli around this time, led Leonhard Euler to the problem of showing that an algebraic equation $P(x) = 0$, where P is a polynomial of degree n with real coefficients,

has n real or complex roots (1749: *Researches on the imaginary roots of equations*).

This theorem is usually known as the "fundamental theorem of algebra". In France, it is known as d'Alembert's theorem, because Jean d'Alembert proposed an interesting but incomplete proof of it in 1746. In his course at the École Normale in the year III of the French Revolution, Pierre Simon de Laplace gave an elegant proof, admitting only the existence of roots *somewhere*. Gauss gave an entirely satisfying proof of the theorem at least four times (in 1797–1799, twice in 1816, and in 1849), as did Jean Argand (1814) and Louis Augustin Cauchy (1820). The fundamental theorem of algebra can also be obtained as an immediate corollary of the theorem known as *Liouville's theorem* (actually due to Cauchy, 1844), which states that "every holomorphic function bounded on $\mathbb{C}$ is constant".

1.7 The Problem of Algebraic Solutions of Equations

This problem is the central subject of this book. Algebraically solving an algebraic equation (or solving it by radicals) means expressing its solutions by means of n-th roots, i.e. reducing its solution to the solution of equations of the form $x^n = a$.

Around 1700 B.C., the Babylonians were already in possession of a general method for solving quadratic equations whose coefficients were given numbers. Solutions to cubic equations came only with Scipio del Ferro (1515), and quartic equations were solved by Lodovico Ferrari (1540).

Ehrenfried Tschirnhaus (1683), followed by Michel Rolle (1699), Etienne Bézout, and Leonhard Euler (1762) attempted to go further, but Euler still believed that all algebraic equations were solvable by radicals "...one will grant me that expressions for the roots do not contain any other operations than extraction of roots, apart from the four vulgar operations, and one could hardly support the position that transcendental operations meddle in the situation" (§77 of the 1749 article cited above).

Around 1770, Joseph Louis Lagrange and Alexandre Vandermonde (as well as Edward Waring) independently discovered the role played by symmetry properties in the solution of equations. We will detail their discoveries in Chapter 10. As for the contribution of Gauss, we mentioned it in §1.3 above.

These ideas were exploited by Paolo Ruffini (1802–1813) to prove the impossibility of solving the general equation of the fifth degree by radicals, and then by Niels Abel (1823–1826) to prove the impossibility of solving the general equation of degree ≥ 5 by radicals (see Chapter 12). However, the analysis of their texts would occupy too much of this book; we refer the reader to the books and articles cited in the introduction to this chapter.

Finally, in 1830, Galois, who knew nothing of Abel's results, created the notions of a group (limited to permutation groups), a normal subgroup, and a solvable group, which allowed him – at least theoretically – to relate the solvability of an equation by radicals to the properties of a group associated to the equation, opening new horizons that are far from having been completely explored even today.

Toward Chapter 2

Before giving a complete exposition of Galois theory in Chapter 4, we devote the following chapter to the history of the solution of algebraic equations through the year 1640.

2

History of the Resolution of Quadratic, Cubic, and Quartic Equations Before 1640

In this chapter, we give only a brief sketch of the rich history of low-degree equations; in particular, we have omitted the Indian and Chinese contributions. Readers interested in the subject can find excellent sources in the bibliography (see, in particular, the books by Tignol, Van der Waerden, and Yushkevich).

2.1 Second-Degree Equations

2.1.1 The Babylonians

The earliest form of writing was invented by the Sumerians in Mesopotamia around 3300 B.C., although some people believe that Egyptian writing was invented earlier. Archaeologists have excavated texts that were written on humid clay tablets later dried in the sun. The earliest known texts are very short and mostly concern accounting: sacks of grain, domestic animals, slaves. They use a numeral system in base 60, which is at the origin of our division – still in use after 5000 years! – of the hour into minutes and seconds and the circle into degrees.

After various historical events, this extraordinary civilization gave way, during the period 1900 to 1600 B.C., to an empire whose capital was Babylon, on the Euphrates, just south of Baghdad today. Quantities of interesting information are preserved in the tablets of this period; in particular, they reveal that Babylonians possessed a well-developed algebra and mastered the solution of second-degree equations.

EXAMPLE. – "I added 7 times the side of my square and 11 times the surface: 6.15" (tablet n° 13901 from the British Museum).

This problem discusses the quadratic equation $11x^2 + 7x = 6.15$; the notation 6.15 in base 60 is ambiguous because the Babylonians gave no indication of the scale: 6.15 could be $6 \times (60)^2 + 15 \times 60$ or $6 \times 60 + 15$, or $6/60 + 15/60^2$, or even $6/3600 + 15$, etc. (A kind of zero, serving to denote the intermediate positions, was introduced by the Babylonians only around 300 B.C. Before that, they sometimes left a space, but more usually it was just necessary to guess. Here, $6.15 = 6 + 15/60 = 6 + 1/4$.)

To follow the solution described in the tablet, set $a = 11$, $b = 7$, and $c = -6\frac{1}{4}$. The two left-hand columns of Table 2.1 are translated directly from the tablet. The table also shows the numbers written in base 10 and the corresponding literal computation. Note that in order to facilitate division, the Babylonians had established tables of inverses. But 1/11 was not in the tables, as it does not have a finite expansion in base 60.

	Base 60	Base 10	Computation of
You will multiply 11 by 6.15	1.8.45	$68 + \frac{3}{4}$	$-ac$
You will multiply 3.30 by 3.30	12.15	$12 + \frac{1}{4}$	$\frac{b^2}{4}$
You will add it to 1.8.45	1.21	81	$\frac{b^2}{4} - ac$
It is the square of	9	9	$\sqrt{\frac{b^2}{4} - ac}$
You will subtract 3.30	5.30	$5 + \frac{1}{2}$	$-\frac{b}{2} + \sqrt{\frac{b^2}{4} - ac}$
The inverse of 11 cannot be computed			
What, multiplied by 11, gives 5.30?	30	$\frac{1}{2}$	$\frac{-\frac{b}{2} + \sqrt{\frac{b^2}{4} - ac}}{a}$
The side of the square is 30.			

TABLE 2.1. Method for solving a quadratic equation

OTHER EXAMPLES. – Here are the equations corresponding to other problems from the same tablet. The numbers in parentheses are the values to be given to the Babylonian numbers:

$$\begin{aligned} x^2 + x &= 45 & &\left(\tfrac{3}{4}\right) \\ x^2 &= x + 14.30 & &(870) \\ x^2 - 20x^2 + x &= 4.46.40 & &\left(\tfrac{1}{3} \quad \text{and} \quad 286 + \tfrac{2}{3}\right). \end{aligned}$$

COMMENTARY. – In these problems, the solutions are always positive numbers having simple finite expansions in base 60: the discriminant is the square of a simple number, and the division by a works. Apart from these restrictions, we see that the Babylonians mastered the algorithm for the algebraic solution of quadratic equations. Even the case of second-degree equations having two distinct positive roots seems to be considered in problems in which the length and width of a rectangle appear, which makes it possible to distinguish numbers that cannot be distinguished algebraically by using an order relation. However, they only wrote on their tablets straightforward recipes to be followed; we have no idea how they actually thought of them. The deductive method in mathematics was invented later, by the Greeks.

2.1.2 The Greeks

The irrationality of $\sqrt{2}$ was proved around 430 B.C., probably by a geometric argument. (The discovery is attributed to Hippasos of Metapont, who supposedly was unable to endure the intellectual consequences of his discovery and drowned himself in the Aegean Sea. At the very least, this anecdote bears witness to the deep trouble provoked by the discovery.)

In Euclid's *Elements* (dating from about 300 B.C.), the methods are geometric; algebraic computations cannot be developed, because a product of two lengths is considered to be a surface. Later, in the 3rd century A.D., Diophantus discovered an algebraic approach.

There is one important difference between the documentation at our disposal on Babylonian and on Greek mathematics: the tablets preserve the original state of Babylonian mathematics, whereas the work of the Greeks is known to us only through manuscripts written a good thousand years after the authors made their discoveries, which reworked the originals in all kinds of ways. Some works are known only from their translations into Arabic.

2.1.3 The Arabs

It is more correct to speak of mathematicians coming from the various provinces of the Arab world, from Spain to the Middle East, than it is to speak directly of "Arab mathematicians". In the 8th century, these mathe-

maticians began to procure Greek texts from Constantinople; they also received Indian books of computations that explained the use of zero. Around 820 to 830, al Khwarizmi (from Uzbekistan; he later became known through Latin translations of his works, called Algorismus, origin of the word algorithm), a member of the scientific community around the caliph al Mamoun, described algebraic transformations in his treatise on algebra, which can be expressed as the following equations in our notation:

$$\begin{aligned} 6x^2 - 6x + 4 &= 4x^2 - 2x + 8 & \\ 6x^2 + 4 + 2x &= 4x^2 + 8 + 6x & \text{by al jabr} \\ 3x^2 + 2 + x &= 2x^2 + 4 + 3x & \text{by al hatt} \\ x^2 &= 2x + 2 & \text{by al muqqabala.} \end{aligned}$$

The word al jabr, which expressed completion or setting of a fracture, is at the origin of the appearance of the word "algebra" in the 14th century.

al Khwarizmi distinguishes six types of equations of degree less than or equal to 2, because the coefficients a, b, and c of his equations are always positive:

$$ax^2 = bx, \qquad ax^2 = b, \qquad ax = b,$$

$$ax^2 + bx = c, \quad ax^2 + c = bx, \quad ax^2 = bx + c.$$

For the equation $x^2 = 40x - 4x^2$, or $x^2 = 8x$, he gives only the root 8. However, for the equation $x^2 + 21 = 10x$, he gives the two solutions 3 and 7 and asserts that the procedure is the same for all equations of the fifth type. Geometric justifications are given, but unlike the Greeks, the spirit of the method is algebraic.

2.1.4 Use of Negative Numbers

Negative numbers became widely used only around the end of the 16th century. However, they actually appeared 1,000 years earlier in Indian mathematics and even earlier than that in Chinese mathematics.

In 1629, following ideas developed by Stevin in 1585, Girard did not scruple to give examples of equations with negative roots: "The negative in geometry indicates a regression, and the positive an advancement" (nor was he bothered by complex non-real roots).

However, one must not believe that negative roots were accepted by everyone: in 1768, Bézout still wrote that equations have negative roots only when they are "vicious", and Lazare Carnot, the famous "organizer of the victory" of the Republican armies, wrote in his treatise on geometry in the year XI of the Revolution: "To obtain an isolated negative quantity, one must remove an effective quantity from zero, but removing something from nothing is an impossible operation."

2.2 Cubic Equations

2.2.1 The Greeks

On the rare occasions in which they encountered cubic equations, the Greeks solved them by means of intersections of conics: ellipses, parabolas, and hyperbolas. The oldest such solution goes back to Menechme (375–325 B.C.), who, to obtain an x such that $x^3 = a^2b$, considered the intersection of $x^2 = ay$ and $xy = ab$ (others expressed the same problem as the search for numbers x and y such that $a/x = x/y = y/b$). The most famous solution, which led to numerous further developments, goes back to Archimedes. He sought to cut a sphere of radius R by a plane in such a way that the ratio of the volumes of the two pieces had a given value k: we easily see that the height h of one of the parts satisfies $h^3 + \big(4k/(k+1)\big)R^3 = 3Rh^2$.

But the Greeks did not solve the problem of the duplication of the cube with ruler and compass (equation $x^3 = 2a^3$), nor the trisection of the angle; we will discuss these questions in Chapter 5.

2.2.2 Omar Khayyam and Sharaf ad Din at Tusi

Omar Khayyam was a mathematician and an astronomer, but he was also a poet, the author of many famous verses. He lived in central Asia and in Iran (1048–1131). In his treatise on algebra (from around 1074), he studied cubic equations in detail. He only considered equations with strictly positive coefficients, and distinguished 25 different cases, some of which had already been studied by al Khwarizmi. For example, the equations with three terms not having zero as a root are of one of the following six forms (Omar Khayyam expresses them in words, without notation, with homogeneity conditions similar to those of §1.4):

$$x^3 = ax^2 + b, \quad x^3 + b = ax^2, \quad x^3 + ax^2 = b,$$

$$x^3 = ax + b, \quad x^3 + b = ax, \quad x^3 + ax = b.$$

For $x^3 + ax = b$, he set $a = c^2, b = c^2h$ and obtained the solution as the intersection of the parabola $y = x^2/c$ and the circle $y^2 = x(h - x)$.

For $x^3 + b = ax$, he again set $a = c^2, b = c^2h$ and obtained the solution as the intersection of the parabola $y = x^2/c$ and the hyperbola $y^2 = x(x - h)$.

One hundred years later, in a treatise that has just been reedited (see the bibliography), Sharaf ad Din at Tusi classified equations, not according to the sign of the coefficients like Khayyam, but according to the existence of strictly positive roots. He solved the homogeneity problems in a manner that appears to foreshadow Descartes (see §5.7): every number x can be identified with a length or with a rectangular surface of sides 1 and x, or even with the volume of a parallelepiped with sides 1, 1 and x. Finally,

he inaugurated the study of polynomials via analysis, introducing their derivative, seeking for their maxima, etc.

The solutions given by Omar Khayyam are geometric, obtained by taking intersections of conics. As for algebraic solutions, he writes that "they are impossible for us and even for those who are experts in this science. Perhaps one of those who will come after us will find them." Similar remarks were made by Luca Pacioli in 1494 but times were changing, because...

2.2.3 Scipio del Ferro, Tartaglia, Cardan

...the work of Italian mathematicians since Leonard of Pisa finally reached a conclusion in 1515. Scipio del Ferro, a professor in Bologna who died in 1526, discovered the algebraic solutions of the equations

$$x^3 + px = q, \tag{2.1}$$

$$x^3 = px + q, \tag{2.2}$$

$$x^3 + q = px, \tag{2.3}$$

probably with $p, q > 0$, i.e. of type (2.1) only. The rest of the story is a novel in episodes which is impossible to reconstruct completely, as many of the details are known only because they were recounted by one of the protagonists, in a manner that may lack objectivity.

In the year 1535, Fiore, a Venitian student of Scipio del Ferro, publicly challenged Niccolà Tartaglia (roughly 1500–1559) to solve about 30 problems, all based on equations of type (2.1). At that time, winning a challenge of this kind led to prestige and money, sometimes even allowing the winner to obtain a position as a professor. Tartaglia's childhood was very dramatic: a fatherless child, very poor, he was seriously wounded during the looting of Brescia by troops led by Gaston de Foix in 1512. He had already attempted to solve equations of this type some years earlier, and this time he succeeded, during the night of February 12 to 13, 1535 (just in time to win the challenge). But he kept his solution secret. He wrote it in a poem, in which he used the word "thing", like his contemporaries, for the unknown.

Quando che'l cubo con le cose appresso
Se agguaglia a qualche numero discreto...,

(When the cube with the things is equal to a number....)

In 1539, Jerôme Cardan, a doctor and mathematician, and a very complex personality whose tumultuous life also makes a highly interesting story, invited Tartaglia to his house in Milan to find out his secret. He flattered him so well that he succeeded – Tartaglia showed him his poem – but swore not to reveal it (March 25, 1539). Shortly after, Cardan succeeded in extending Tartaglia's method to equations of types (2.2) and (2.3) (unless it was actually Tartaglia who succeeded), and one of his disciples, Ferrari (1522–1560), solved the quartic equation in 1540.

In 1545, Cardan published all of these solutions in his book *Ars Magna* (which literally means: *Grand Work*), taking care to thank Tartaglia three times. But Tartaglia was furious, denounced him for lying, and the following year published a text containing Cardan's promise, their conversations together, and his own research. Ferrari defended his professor, saying that he had been present at the meeting in 1539 and that there was never any question of a secret. He then took up a new challenge proposed by Tartaglia on August 10, 1548, which he appears to have won. And the story continued.

Cardan's *Ars Magna* is a very important book. In it, he gave the complete solution of the cubic equation, finally (see, however, §2.2.5), as well as the first computations using roots of negative numbers.

2.2.4 Algebraic Solution of the Cubic Equation

In 1545, Cardan explained on the basis of numerous numerical examples, which he considered as clearly illustrating the general case, how to find a root of the cubic equation. The problem of finding the three roots was solved by Euler, in a Latin article from 1732.

Let us explain Cardan's method, using today's notation and without distinguishing the different cases due to signs of the coefficients, as Cardan did. We know that by translation, we can always reduce to the case of an equation of the form $x^3 + px + q = 0$.

Set $x = u + v$ (for Cardan, this is either $u + v$ or $u - v$ according to the signs of p and q), and require the numbers u and v to satisfy the condition $3uv = -p$. The equation can be written as

$$(u+v)^3 + p(u+v) + q = 0; \qquad \text{or as} \qquad u^3 + v^3 + (u+v)(3uv+p) + q = 0,$$

so setting $3uv = -p$, this gives

$$u^3 + v^3 = -q, \qquad u^3v^3 = -\frac{p^3}{27}.$$

Setting $U = u^3$ and $V = v^3$, this then gives

$$U + V = -q, \qquad UV = -\frac{p^3}{27},$$

so that U and V are solutions of the quadratic equation $X^2 + qX - p^3/27 = 0$. The discriminant of this quadratic equation is given by

$$\frac{q^2}{4} + \frac{p^3}{27}.$$

If d is a number whose square is equal to this discriminant, then setting $U = -(q/2) + d$ and $V = -(q/2) - d$ gives a solution.

Cardan concludes his procedure by giving the unique solution $x = \sqrt[3]{U} + \sqrt[3]{V}$, i.e.

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

This formula requires the extraction of two cube roots (really just one since $v = -p/3u$).

For us, this formula contains an ambiguity: each of the cube roots can be chosen in three different ways, and their sum could have nine different values. Let us now redo the method, considering the cube roots as Euler did.

If u satisfies $u^3 = U$, then the condition $3uv = -p$ implies that $v = -p/3u$, giving the solution

$$x = u + v$$

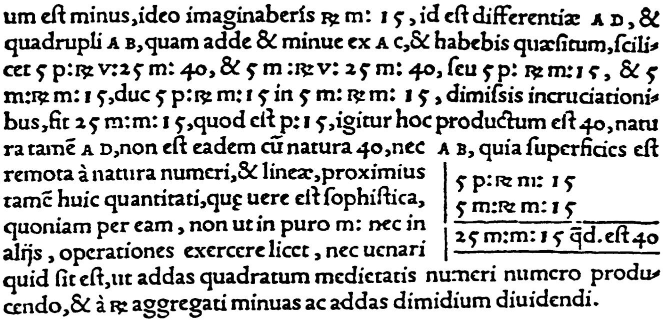
of the equation. The other cube roots of U are ju and j^2u, corresponding to $-p/3ju = j^2v$ and $-p/3j^2u = jv$ respectively; here j is a cube root of unity, i.e. $j = \exp(2\pi/3)$. This gives the other solutions of the equation

$$ju + j^2v, \qquad j^2u + jv.$$

If we reverse the choices of U and V, a cube root of $-q/2 - d$ is one of the three numbers above v, jv, j^2v, and fortunately, we find the same three roots.

2.2.5 First Computations with Complex Numbers

The spark occurs near the end of the *Ars Magna*, in 1545 (Figure 2.1). The idea was undoubtedly suggested to Cardan by the problems he studied in dealing with cube roots as above.


um eſt minus, ideo imaginaberis ℞ m: 15, id eſt differentiæ A D, & quadrupli A B, quam adde & minue ex A C, & habebis quæſitum, ſcilicet 5 p: ℞ v: 25 m: 40, & 5 m: ℞ v: 25 m: 40, ſeu 5 p: ℞ m: 15, & 5 m: ℞ m: 15, duc 5 p: ℞ m: 15 in 5 m: ℞ m: 15, dimiſsis incruciationibus, fit 25 m: m: 15, quod eſt p: 15, igitur hoc productum eſt 40, natura tamē A D, non eſt eadem cū natura 40, nec A B, quia ſuperficies eſt remota à natura numeri, & lineæ, proximius tamē huic quantitati, quę uere eſt ſophiſtica, quoniam per eam, non ut in puro m: nec in alijs, operationes exercere licet, nec uenari quid ſit eſt, ut addas quadratum medietatis numeri numero producendo, & à ℞ aggregati minuas ac addas dimidium diuidendi.

5 p: ℞ m: 15
5 m: ℞ m: 15
25 m: m: 15 q̄d. eſt 40

FIGURE 2.1. Excerpt from the book *Ars Magna* by Cardan, 1545

This excerpt refers to the search for two numbers whose sum is 10 and whose product is 40, leading to the equation $x^2 - 10x + 40 = 0$. Cardan

recognized that no two numbers could satisfy this equation, but proposed a *sophisticated* solution in which he *imagined* the number $\sqrt{-15}$; he then checked the validity of this number by computing

$$\left(5+\sqrt{-15}\right)\left(5-\sqrt{-15}\right)=25-(-15)=40,$$

writing this operation as

5 p : ℞ m : 15,
5 m : ℞ m : 15,
25 m : m 15 q̃d. est 40,

where p denotes +, m denotes −, and ℞ denotes the square root. One passage provoked a great deal of commentary: *dimissis incruciationibus*, which means *setting aside the products in crosses*, or, according to certain translators who think Cardan is making a word play, *setting aside the mental torture.*

In the case of the cubic equation, complex numbers enter in the case when $q^2/4+p^3/27<0$, known as the irreducible case, in which the three roots are real (see §3.6) and d is purely imaginary. Cardan did not understand this case well; he simply showed how to obtain all three roots if one of them is known (see Exercise 2.4).

2.2.6 Raffaele Bombelli

Born in 1530, Bombelli published a treatise on algebra in 1572 which improved understanding of computations with complex numbers by showing how Cardan's formulas can be applied in the irreducible case. He gave numerous examples; one of the simplest is that of the equation which we write as $x^3-15x-4=0$, which has an obvious solution 4, knowing which Cardan's formulas produce the quantities $\sqrt[3]{2\pm\sqrt{-121}}$. Now, this is the irreducible case since $d^2=q^2/4+p^3/27=4-125=-121$ and $u^3=U=-q/2+d=2+\sqrt{-121}$.

Bombelli explained this difficulty by showing that $\sqrt[3]{2+\sqrt{-121}}$ can actually be written in the form $a+ib$; identifying the real parts of $(a+ib)^3$ and $2+11i$, he found $a^3-3ab^2=2$. The equality of the modules then gave $(a^2+b^2)^3=(2^2+11^2)=125$, so $a^2+b^2=5$. He then substituted $b^2=5-a^2$ into the previous equation, obtaining $a^3-3a(5-a^2)=4a^3-15a=2$ (this is the original equation with $x=2a$). Bombelli noticed that $a=2$ is a root, and deduced that $b=1$, giving $u=2+i, v=2-i$, and $u+v=4$ (with notation as in §2.2.5 above). Abraham de Moivre (1667–1754) later observed that this procedure requires having already solved the equation to simplify the expression of the roots. Nonetheless, Bombelli's work is extremely important: it opened the way to computations with complex numbers.

Bombelli's notation is Rc ⌊2p dim 11⌋: the cube root of the quantity between the signs ⌊ and ⌋, which is the abbreviation of of "2 pi di meno 11", where "pi di meno n" means $+in$. Bombelli gave rules such that:

pi di meno via pi di meno fa meno,
pi di meno via meno di meno fa pi, etc.

corresponding to $(+i)(+i) = -1, (+i)(-i) = 1$, etc.

2.2.7 François Viète

In a text published after his death, in 1615, Viète gave solutions of equations of degree 3 and 4. For the cubic equation

$$A^3 + 3BA = 2Z,$$

which we write here with our notation, but using his original letters, with A as the unknown, he introduced a new unknown E such that $EB = E(A+E)$, which comes down to solving the equation $x^3 + px + q = 0$ with the variable change $x = (p/3y) - y$, giving

$$A^3 + 3AE(A+E) = 2Z, \qquad (A+E)^3 = 2Z + E^3, \qquad B^3 = 2ZE^3 + E^6,$$

a quadratic equation in E^3. This makes it possible to compute E, then A, by means of a single extraction of a cube root; the method is essentially Cardan's.

2.3 Quartic Equations

Cardan gave a method for these equations in Chapter XXXIX of the *Ars Magna*; he says that it was discovered by his student Lodovico Ferrari. It consists in using a translation to bring the equation to the form

$$x^4 + px^2 + qx + r = 0$$

(Cardan, who rejected negative numbers, only gives a few cases of this).

Set $z = x^2 + y$, obtaining

$$z^2 = x^4 + 2x^2y + y^2 = -px^2 - qx - r + 2x^2y + y^2 = (2y-p)x^2 - qx + y^2 - r.$$

Choose y so that the right-hand term is of the form $(Ax+B)^2$, by ensuring that its discriminant vanishes, i.e.

$$q^2 - 4(y^2 - r)(2y - p) = 0. \qquad (*)$$

This gives a cubic equation (which later came to be called a *resolvent*); one of its roots can be found by the method of §2.2.4, giving

$$(x^2 + t)^2 = (Ax + B)^2, \qquad x^2 = -t \pm (Ax + B),$$

and four values for x.

In the case where the right-hand term is not of degree 2, it is because $y = p/2$, and then (*) shows that $q = 0$; the equation is biquadratic, which we know how to solve.

In his 1615 text, François Viète gave a clear exposition of Ferrari's method.

Cardan detested introducing equations of degree higher than 3, because equations of degrees 1, 2, and 3 concerned segments, areas, and volumes and he asserted that "nature does not allow us to consider others".

Here is another method, using indeterminate coefficients, which dates back at least to Descartes (1637). If a, b, c, d are such that

$$x^4 + px^2 + qx + r = (x^2 + ax + b)(x^2 + cx + d),$$

we check (see Exercise 2.7) that a^2 is the root of a cubic equation and that b, c, d depend rationally on a.

Exercises for Chapter 2

Exercise 2.1. Irrationality of roots of rational numbers

Let $k > 1$ be an integer, and let a and b be positive relatively prime integers with no factors of the form d^k for integers $d > 1$. Show that $\sqrt[k]{\frac{a}{b}}$ is not a rational number.

Exercise 2.2. Cubic equations and Cardan's formulas

1) Solve the equations $x^3 + 3x = 10, x^3 + 21x = 9x^2 + 5, x^3 = 7x + 7$ by Cardan's method or Viète's method.

2) Simplify the following expressions, where the roots are taken in $\mathbb{R}$, and compare them with Cardan's formulas.

$$\alpha = \sqrt[3]{10 + \sqrt{108}} + \sqrt[3]{10 - \sqrt{108}}, \qquad \beta = \sqrt[3]{1 + \frac{2}{3}\sqrt{\frac{7}{3}}} + \sqrt[3]{1 - \frac{2}{3}\sqrt{\frac{7}{3}}}.$$

Exercise 2.3. Simplification of radicals in Cardan's formulas

If a cubic equation has an integral root, it often happens that Cardan's formula gives an expression with cube roots whose simplification is not at all obvious. Tartaglia already noticed this problem in 1540, and we showed earlier how Bombelli worked on one example (see §2.6). Let us consider what happens in the case of equations with rational coefficients.

1) Show that if we have $p, q, r, s \in \mathbb{Q}$ such that $q, s > 0$ and q is not a square in $\mathbb{Q}$, then the equality $p + \sqrt{q} = r + \sqrt{s}$ implies that $p = r$ and $q = s$.

2) Let a and b be rational numbers such that $b > 0$ is not a square in $\mathbb{Q}$. Suppose there exist rational numbers y and z such that $\sqrt[3]{a + \sqrt{b}} = y + \sqrt{z}$.

a) Show that $\sqrt[3]{a - \sqrt{b}} = y - \sqrt{z}$.

b) Show that $c = \sqrt[3]{a^2 - b}$ is rational.

c) Show that the equation $x^3 - 3cx - 2a = 0$ has a unique rational root (use §3. 6. 4 below); compute y and z in terms of this root and c.

3) Conversely, if the equation $x^3 - 3cx - 2a = 0$, with rational coefficients, has a rational root and two non-real roots, show that there exist rationals y and z such that $\sqrt[3]{a + \sqrt{b}} = y + \sqrt{z}$, where $b = a^2 - c^3 > 0$.

4) Does this result make it possible to simplify the expression given by Cardan's formulas for the roots of $x^3 + px + q = 0$ (with p and q rational), when one of the roots is rational and the others are non-real?

5) Simplify the following expressions, using the above; all roots are taken in $\mathbb{R}$:

$$\sqrt[3]{10 + \sqrt{108}}, \qquad \sqrt[3]{10 - \sqrt{108}}, \qquad \sqrt[3]{1 + \frac{2}{3}\sqrt{\frac{7}{3}}}, \qquad \sqrt[3]{1 - \frac{2}{3}\sqrt{\frac{7}{3}}}.$$

Exercise 2.4. Cubic equations, irreducible case, Cardan's method

This problem concerns the solution of the equation $x^3 + px + q = 0$ in the case where p and q are real and the discriminant is ≥ 0. The equation has three real roots but Cardan's formulas lead to roots of non-real numbers.

1) Let a be a solution of the equation. Compute the other two solutions as functions of a and p.

2) Check the following text by Cardan for the solution of $x^3 + 60 = 46x$:

"A solution is 6. To find the others, raise 3, half of the first solution, to the square; this gives 9 which, multiplied by 3, gives 27. Subtract 27 from 46, leaving 19. Subtract 3, half of the first solution, from the square root of this number: you obtain the second solution $\sqrt{19} - 3$. By the same method, if you found $\sqrt{19} - 3$ as a first solution, the other solution will be 6."

Exercise 2.5. Cubic equation, irreducible case, Viète's method

This problem concerns the solution of the equation $x^3 + px + q = 0$ in the case where p and q are real and the discriminant is ≥ 0.

1) Show that we can reduce to an equation of the form $y^3 - 3y = 2u$, with $u \in \mathbb{R}$ and $|u| \leq 1$.

2) Solve this equation by setting $v = \arccos u$.

3) Solve $X^3 - 6X - 4 = 0$ by this method.

COMMENTARY. – Viète's method shows the relation between the irreducible case and the trisection of the angle (there is an analogy with the method of Charles Hermite for equations of degrees 5 and 6, based on the division of elliptic functions). In the example in 3), Cardan's formulas lead to radicals of non-real numbers.

Exercise 2.6. Seventh roots of unity

Set $\zeta = e^{2i\pi/7}$ and $\alpha = 2\cos\dfrac{2\pi}{7}$.

1) Give a quadratic equation satisfied by ζ over $\mathbb{Q}[\alpha]$.

2) Find an irreducible cubic polynomial in $\mathbb{Q}[X]$ which admits α as a root.

Exercise 2.7. Quartic equation and Descartes' method

By translation, we first reduce to the case of a quartic equation with no third-degree term

$$x^4 + px^2 + qx + r = 0.$$

Then, if this equation has a linear term, we look for a factorization of the form

$$x^4 + px^2 + qx + r = (x^2 + ax + b)(x^2 + cx + d).$$

1) Show that a^2 is a root of a cubic equation and that b, c, d are rational functions of a.

2) Deduce the algebraic solution of the quartic equation from this.

3) Solve

$$\begin{aligned} x^4 - 4x^2 - 8x + 35 &= 0, \\ x^4 - 17x^2 - 20x - 6 &= 0. \end{aligned}$$

4) Show that if p, q, r are real, we can choose a, b, c, d real.

COMMENTARY. – Let us quote Descartes: "Au reste, j'ai omis ici les démonstrations de la plupart de ce que j'ai dit, à cause qu'elles m'ont semblé si faciles que, pourvu que vous preniez la peine d'examiner méthodiquement si j'ai failli, elles se présenteront à vous d'elles-mêmes; et il sera plus utile de les apprendre en cette façon qu'en les lisant."[1]

The examples in 3) are those of Descartes. Question 4) is a result of Euler (1749) in his work on the decomposition of polynomials in $\mathbb{R}[X]$ into products of linear or quadratic factors.

Solutions to Some of the Exercises

Solution to Exercise 2.1.

If there exist positive and relatively prime integers x and y such that $x/y = \sqrt[k]{a/b}$, then we have $bx^k = ay^k$. As x is prime to y, it must divide a, so $x = 1$. Similarly, $y = 1$ and we are done.

Solution to Exercise 2.2.

1) To solve the equation $x^3+px+q = 0$, we know that we need to determine u and v such that $u^3 + v^3 = -q$ and $uv = -p/3$, and then set $x = u + v$, $ju + j^2v$, $j^2u + jv$.

For $x^3 + 3x - 10 = 0$, we obtain $u = \sqrt[3]{5 + \sqrt{26}}$, $v = \sqrt[3]{5 - \sqrt{26}}$ (the roots are taken in $\mathbb{R}$).

For $x^3 + 21x = 9x^2 + 5$, we set $y = x - 3$, which leads to solving the equation $y^3 + 4 = 6y$; we obtain the root $y = 2$ and then divide by $y - 2$, avoiding the extraction of cube roots. Like Cardan, we find three real roots, namely $x = 5$ and $x = 2 \pm \sqrt{3}$.

For $x^3 - 7x - 7 = 0$, we obtain

$$u = \sqrt[3]{7/2 + 7i/18\sqrt{3}} \quad \text{and} \quad v = \sqrt[3]{7/2 - 7i/18\sqrt{3}},$$

where the arguments of the cube roots are chosen with opposite signs, since we must have $uv = 7/3$.

2) To find the equation having α as a root, we can compute α^3 and compare it with α. We can also compare the form of α with the general solution of

[1] Besides, I left out the proofs of most of what I said here, because they appeared so easy to me that if you just take the trouble to check methodically whether I erred, they will present themselves to you naturally, and it will be more useful to you to learn them this way than by reading them.

the cubic equation, which leads us to set $q = -20$; then $108 = q^2/4 + p^3/27$ gives $p = 6$. The equation $x^3 + 6x - 20 = 0$ has 2 as a root, so when we divide it by $(x - 2)$, we obtain the other roots $-1 \pm 3i$. The only real root is 2, so we find that $\alpha = 2$.

Similarly, we find $\beta = 1$.

Solution to Exercise 2.4.

1) We have $x^3 + px + q = (x - a)(x^2 + ax + p + a^2)$. The roots of the second factor are real; they are given by $-\frac{a}{2} \pm \sqrt{-3(\frac{a}{2})^2 - p}$.

2) Cardan uses his formula on his example with the sign + for the root. To check the last sentence, we set $a = \sqrt{19} - 3$ and note that $-3(a/2)^2 - p = \left((9 + \sqrt{19})/2\right)^2$.

COMMENTARY. – Cardan gave no general method for this type of equation; he did not use his formula and could only guess at one root in order to find solutions for the remaining quadratic equation.

Solution to Exercise 2.5.

1) Setting $x = \alpha y$, we are led to take $\alpha = \sqrt{-p/3}$, so that $2u = -q/\alpha^3$; we then check that $|u| \leq 1$.

2) The formula $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ gives

$$2\cos v/3, \quad 2\cos\left((v/3) + (2\pi/3)\right), \quad 2\cos\left((v/3) + (4\pi/3)\right)$$

as roots of the equation $y^3 - 3y = 2\cos v$.

3) We find $\alpha = \sqrt{2}$, $u = \sqrt{2}/2$, $v = \pi/4$ and the roots are

$$a = 2\sqrt{2}\cos\frac{\pi}{12}, \qquad b = 2\sqrt{2}\cos\frac{3\pi}{4} = -2, \qquad c = 2\sqrt{2}\cos\frac{17\pi}{12}.$$

Since -2 is a root, we can also write $x^3 - 6x - 4 = (x + 2)(x^2 - 2x - 2)$, which gives $a = 1 + \sqrt{3}$, $c = 1 - \sqrt{3}$.

Solution to Exercise 2.6.

1) ζ is a root of the quadratic equation $x^2 - \alpha x + 1 = 0$.

2) We have the equation $\alpha^3 + \alpha^2 - 2\alpha - 1 = 0$, of which 1 and -1 are not roots.

Solution to Exercise 2.7.

1) By identification, we successively find

$$a + c = 0 \tag{2.4}$$
$$ac + b + d = p \tag{2.5}$$
$$ad + bc = q \tag{2.6}$$
$$bd = r. \tag{2.7}$$

We deduce that $c = -a$, $b + d = p + a^2$ and $a(d - b) = q$. Thus $a \neq 0$ since $q \neq 0$, so we obtain $b + d$ and $b - d$, which gives b and d; plugging them into (2.7) gives

$$(ap - q + a^3)(ap + q + a^3) = 4ra^2, \tag{2.8}$$
$$a^6 + 2pa^4 + (p^2 - 4r)a^2 - q^2 = 0. \tag{2.9}$$

The last equation is a cubic in a^2 (it is a resolvent, corresponding to the choice of $-u$, $-v$, $-w$ in §10.8 below). We obtain six values of a, each of which gives a factorization. This is normal since a is the sum of two of the four roots of the equation and $\binom{4}{2} = 6$.

2) Once the factorization is obtained, it remains only to solve quadratic equations.

3) With $a = 4$, we have

$$X^4 - 4X^2 - 8X + 35 = (X^2 - 4X + 5)(X^2 + 4X + 7),$$
$$X^4 - 17X^2 - 20X - 6 = (X^2 - 4X - 3)(X^2 + 4X + 2);$$

the rest is easy.

4) The resolvent must have a positive real root since the value of the left-hand side of (2.9) is < 0 for $a = 0$ and > 0 for a sufficiently large.

3
Symmetric Polynomials

In this chapter, we first give the basics on symmetric polynomials, and then present the notions of resultant and discriminant.

3.1 Symmetric Polynomials

3.1.1 Background

Let A be a commutative ring with unit. The A-algebra $A[X_1, \ldots, X_n]$ of polynomials in n indeterminates and coefficients in A has the following universal property: for every A-algebra B given by a ring homomorphism $f : A \to B$ and every map $h : \{1, \ldots, n\} \to B$, there exists a unique homomorphism of A-algebras $\varphi : A[X_1, \ldots, X_n] \to B$ such that $\varphi(X_i) = h(i)$ for all i in $\{1, \ldots, n\}$, and $\varphi(a) = f(a)$ for all a in A. In other words, the universal property asserts that in order to construct a homomorphism φ of A-algebras from $A[X_1, \ldots, X_n]$ to another A-algebra, it suffices to give the images of the indeterminates, and there is nothing further to check.

In the case where $n = 1$ (we denote the indeterminate by X) and the map h is defined by $h(1) = b$, the homomorphism $\varphi : A[X] \to B$ is defined by

$$\varphi\left(\sum a_k X^k\right) = \sum f(a_k) b^k.$$

For every element σ of the group S_n of permutations of the set $\{1, \ldots, n\}$, the above remarks prove that there exists a unique homomorphism of A-algebras $\varphi_\sigma : A[X_1, \ldots, X_n] \to A[X_1, \ldots, X_n]$ (often simply denoted by σ)

making the diagram in Figure 3.1 commutative (the notation "can" means that the arrows are canonical).

In other words, $\varphi_\sigma(X_i) = X_{\sigma(i)}$ for $i = 1, \ldots, n$, and more generally,

$$\varphi_\sigma(P(X_1, \ldots, X_n)) = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

If A is an integral domain with fraction field K, the homomorphism φ_σ extends to the field $K(X_1, \ldots, X_n)$ of rational functions in $X_1, \ldots, X_n$ with coefficients in K. Recall that an element of this field is represented by the quotient of two polynomials in $A[X_1, \ldots, X_n]$, with denominator not equal to zero.

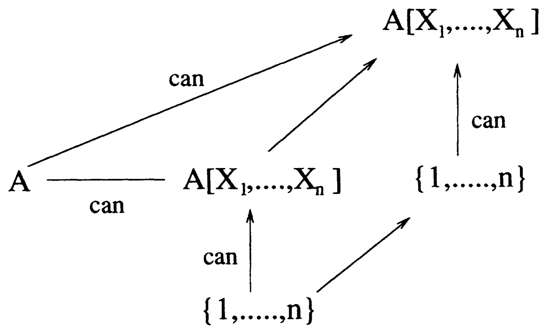


FIGURE 3.1.

3.1.2 Definitions

A polynomial in $A[X_1, \ldots, X_n]$ is said to be *symmetric* if for all σ in S_n, we have $\varphi_\sigma(P) = P$.

If A is an integral domain with fraction field K, a rational function P/Q in the field $K(X_1, \ldots, X_n)$, with $P, Q \in A[X_1, \ldots, X_n]$ and $Q \neq 0$, is said to be *symmetric* if for all σ in S_n, we have $\varphi_\sigma(P/Q) = P/Q$.

EXAMPLES. – The following polynomials are symmetric in $A[X_1, X_2, X_3]$:

$$X_1 + X_2 + X_3,$$

$$X_1X_2X_3,$$

$$X_1^3X_2 + X_2^3X_3 + X_3^3X_1 + X_2^3X_1 + X_3^3X_2 + X_1^3X_3,$$

but $X_1^3X_2 + X_2^3X_3 + X_3^3X_1$ is not.

REMARKS. – The symmetric polynomials generate an A-subalgebra of the algebra $A[X_1, \ldots, X_n]$.

If a polynomial P in $A[X_1, \ldots, X_n]$ is symmetric and if $a(X_1)^{k_1} \ldots (X_n)^{k_n}$ is a monomial in P, then for all σ in S_n, $a(X_{\sigma(1)})^{k_1} \ldots (X_{\sigma(n)})^{k_n}$ is a monomial of P.

3.2 Elementary Symmetric Polynomials

3.2.1 Definition

Let n be an integer ≥ 0. For every integer $k \leq n$, the *elementary symmetric polynomial* of degree k in $A[X_1, \ldots, X_n]$, which we denote by s_k, is given by the formula

$$s_k = \sum_{H \subset \{1,\ldots,n\}, |H|=k} \left(\prod_{i \in H} X_i \right).$$

In other words, H runs over the set of subsets of k elements of $\{1, \ldots, n\}$ and s_k is the sum of the products of the X_i for i in H. For $k > n$, we set $s_k = 0$.

EXAMPLES. – For $n = 0 : s_0 = 1$ and $s_k = 0$ for $k \geq 1$.
For $n = 1 : s_0 = 1$, $s_1 = X_1$, $s_k = 0$ for $k \geq 2$.
For $n \geq 2 : s_0 = 1$; $s_1 = \sum_{1 \leq i \leq n} X_i$; $s_2 = \sum_{1 \leq i < j \leq n} X_i X_j$. Thus, s_2 is just the sum of the products of pairs of X_i. More generally, s_k is the sum of the products of k of the X_i for $k \leq n$, and in particular,

$$s_n = \prod_{1 \leq i \leq n} X_i.$$

REMARKS. – In general, the integer n is implied by the context and we will not give it explicitly.

The s_k are homogeneous polynomials, i.e. polynomials all of whose monomials are of the same degree, namely k.

3.2.2 The Product of the $X - X_i$; Relations Between Coefficients and Roots

PROPOSITION. –

1) *For all $n \geq 0$, we have*

$$\prod_{1 \leq i \leq n} (X - X_i) = \sum_{0 \leq k \leq n} (-1)^k s_k(X_1, \ldots, X_n) X^{n-k} \tag{3.1}$$

in the ring $\mathbb{Z}[X_1, \ldots, X_n][X]$.

2) *If $P(X) = \sum_{0 \leq k \leq n} a_k X^k$ is a monic polynomial of degree n with roots $x_1, \ldots, x_n$ belonging to a field K, then $a_{n-k} = (-1)^k s_k(x_1, \ldots, x_n)$ for $0 \leq k \leq n$.*

PROOF. –

1) Let us show it by induction on n. The formula holds for $n = 0, 1$.

   Suppose it holds for an integer n; let s_k denote the elementary symmetric polynomials in $\mathbb{Z}[X_1, \ldots, X_n]$ and t_k those in $\mathbb{Z}[X_1, \ldots, X_{n+1}]$. We have

$$\begin{aligned}\prod_{1\le i\le n+1}(X - X_i) &= \left[\prod_{1\le i\le n}(X - X_i)\right](X - X_{n+1})\\ &= \left[\sum_{0\le k\le n}(-1)^k s_k X^{n-k}\right](X - X_{n+1})\\ &= \sum_{0\le k\le n}(-1)^k s_k X^{n-k+1} - \sum_{0\le k\le n}(-1)^k s_k X^{n-k} X_{n+1}\\ &= X^{n+1} + \sum_{1\le k\le n}(-1)^k[s_k + s_{k-1}X_{n+1}]X^{n+1-k}\\ &\qquad +(-1)^{n+1} s_n X_{n+1}.\end{aligned}$$

   On the one hand, $s_n X_{n+1} = t_{n+1}$. On the other hand, for $1 \le k \le n$, separating the parts with k elements of $\{1, \ldots, n+1\}$ into those that contain $n+1$ and those that do not, we see that $s_k + s_{k-1}X_{n+1} = t_k$. This gives the desired result.

2) By the universal property of $\mathbb{Z}[X_1, \ldots, X_n]$, there exists a homomorphism $\varphi : \mathbb{Z}[X_1, \ldots, X_n][X] \to K[X]$ such that $\varphi(X) = X$ and $\varphi(X_i) = x_i$ for $1 \le i \le n$. Since

$$P(X) = \varphi\left(\prod_{1\le i\le n}(X - X_i)\right),$$

   we obtain $a_{n-k} = (-1)^k s_k(x_1, \ldots, x_n)$ for $0 \le k \le n$. ◇

EXAMPLES. – Let x_1, x_2, x_3 denote the roots of the polynomial $X^3 + aX^2 + bX + c$. We have

$$\begin{aligned} x_1 + x_2 + x_3 &= -a,\\ x_1x_2 + x_2x_3 + x_3x_1 &= b,\\ x_1x_2x_3 &= -c.\end{aligned}$$

The analogous formulas for second-degree polynomials are well known.

3.3 Symmetric Polynomials and Elementary Symmetric Polynomials

3.3.1 Theorem

Let A be a commutative ring with unit (in particular, our result will hold for fields), and let P be a symmetric polynomial in $A[X_1, \ldots, X_n]$. Then there exists a unique polynomial T of $A[X_1, \ldots, X_n]$ such that $T(s_1, \ldots, s_n) = P$.

EXAMPLES. – 1) $X_1^2 + X_2^2 = (X_1 + X_2)^2 - 2X_1X_2 = T(s_1, s_2)$ in $\mathbb{Z}[X_1, X_2]$ with $T(s_1, s_2) = s_1^2 - 2s_2$.

2) $X_1^3X_2 + X_1X_2^3 = X_1X_2(X_1^2 + X_2^2) = s_1^2s_2 - 2s_2^2$.

COMMENTARY. – After the remarks of Girard and Newton (see §3.4), this result was used freely throughout the 18th century; Lagrange called it "obvious in itself". It appears to have been stated and proved independently by Waring and Vandermonde in 1770. This theorem can be considered as a small part of the results of §8.5.

PROOF. –

1) We prove the existence of the polynomial T by giving an algorithm to compute it.

To begin with, note that it suffices to show the result for symmetric polynomials $S(M)$ defined by a monomial $M = (X_1)^{k_1} \ldots (X_n)^{k_n}$, by setting

$$S(M) = \sum_{U \in A(M)} U \text{ with } A(M) = \{\varphi_\sigma(M), \sigma \in S_n\},$$

since every symmetric polynomial is a linear combination of such polynomials.

So let P be a symmetric polynomial defined by a monomial as above. Choose a total ordering Ω on the set of indeterminates $\{X_1, \ldots, X_n\}$, for example $X_1 > \cdots > X_n$, and order the set of monomials of P according to the lexicographical order on the n-tuples of powers, i.e.

$$(X_1)^{k_1} \ldots (X_n)^{k_n} > (X_1)^{l_1} \ldots (X_n)^{l_n}$$

if there exists $r < n$ such that for $i \leq r$, $k_i = l_i$ and $k_{r+1} > l_{r+1}$.

For example, $(X_1)^2(X_2)^2X_3 > (X_1)^2X_2(X_3)^2 > X_1X_2(X_3)^3 > (X_3)^5$.

For monomials M, M', N, N', we easily see that $M \geq M'$ for Ω implies that $MN \geq M'N$, and this implies the following property:

if $M \geq M'$ and $N \geq N'$, then $MN \geq M'N'$, since $MN \geq M'N \geq M'N'$.

Let $M = (X_1)^{k_1} \dots (X_n)^{k_n}$ be the largest monomial of P for the ordering Ω. We have $k_1 \geq \dots \geq k_n$, since otherwise the transposition exchanging two indices i and j such that $i < j$ and $k_i < k_j$ would transform M into another monomial of P larger than M.

Consider a polynomial of the form $(s_1)^{l_1} \dots (s_n)^{l_n}$. In this product, according to the above property, the largest monomial for Ω is the product of the largest monomials of $s_1, \dots, s_n$, raised to the powers $l_1, \dots, l_n$, i.e. if we have

$$(X_1)^{l_1}(X_1X_2)^{l_2} \dots (X_1 \dots X_n)^{l_n} = X_1^{l_1+\dots+l_n} X_2^{l_2+\dots+l_n} \dots X_n^{l_n}.$$

This monomial will be equal to M if $k_1 = l_1+\dots+l_n$, $k_2 = l_2+\dots+l_n$, etc., i.e. if

$$\begin{aligned} l_n &= k_n, \\ l_{n-1} &= k_{n-1} - k_n, \\ &\dots \\ l_1 &= k_1 - k_2. \end{aligned}$$

Set $P_1 = P - (s_1)^{l_1} \dots (s_n)^{l_n}$, where the l_i have the above values; P_1 is a symmetric polynomial that is either zero or whose largest monomial for Ω is strictly less than M.

If P_1 is zero, we have written P in the desired form

$$P(X_1, \dots, X_n) = T(s_1, \dots, s_n),$$

where T is defined by $T(X_1, \dots, X_n) = (X_1)^{l_1} \dots (X_n)^{l_n}$. Otherwise, P_1 is a linear combination of polynomials of the form $S(M)$ and we start the same procedure for each of them, until we obtain the zero polynomial and the desired expression of P (see the example below).

2) Let us now prove the uniqueness of T. Suppose there exists a non-zero polynomial T in E such that $T(s_1, \dots, s_n) = 0$.

There exist two monomials in T, say

$$M = a(X_1)^{l_1} \dots (X_n)^{l_n} \text{ and } N = b(X_1)^{m_1} \dots (X_n)^{m_n},$$

such that the n-tuples $(l_i)_{1 \leq i \leq n}$ and $(m_i)_{1 \leq i \leq n}$ are different.

Consider the polynomials $M(s_1, \dots, s_n)$ and $N(s_1, \dots, s_n)$. Their largest monomials in $X_1, \dots, X_n$ are

$$a(X_1)^{l_1+\dots+l_n} \dots (X_n)^{l_n} \quad \text{and} \quad b(X_1)^{m_1+\dots+m_n} \dots (X_n)^{m_n};$$

they have n-tuples with different exponents.

It follows that there exists a unique monomial M of T giving the largest monomial in $X_1, \dots, X_n$ of $T(s_1, \dots, s_n)$, which contradicts the hypothesis $T(s_1, \dots, s_n) = 0$. ◇

EXAMPLE. – Let us express

$$P(X,Y,Z) = Y^3Z + YZ^3 + Z^3X + ZX^3 + X^3Y + XY^3$$

in terms of the elementary symmetric polynomials of $\mathbb{Z}[X,Y,Z]$. First, we have

$$s_1 = X + Y + Z, \quad s_2 = XY + YZ + ZX, \quad s_3 = XYZ.$$

If we select the order $X > Y > Z$, then the largest monomial of P is X^3Y, which leads to setting $P_1 = P - s_1^2 s_2$. After doing the computations, we obtain

$$P_1(X,Y,Z) = -5(X^2YZ + XY^2Z + XYZ^2) - 2(X^2Y^2 + Y^2Z^2 + Z^2X^2).$$

The largest monomial of P_1 is X^2Y^2, which is indeed less than X^3Y. Because P_1 is a linear combination of two polynomials of the type defined above, we can work on each of them separately. The first part is clearly equal to $-5s_1s_3$ (which is given immediately by the algorithm); for the second part, we form $X^2Y^2 + Y^2Z^2 + Z^2X^2 - (s_2)^2$, etc. After all computations, we obtain

$$P = s_1^2 s_2 - s_1 s_3 - 2s_2^2.$$

The extension of Theorem 3.3.1 to rational symmetric functions is easy; it is the object of the following proposition.

3.3.2 Proposition

Let A be an integral domain, and let P, Q be polynomials in $A[X_1,\dots,X_n]$, with $Q \neq 0$, such that P/Q is a symmetric rational function. Then there exist polynomials S and T in $A[X_1,\dots,X_n]$ such that

$$\frac{S(s_1,\dots,s_n)}{T(s_1,\dots,s_n)} = \frac{P}{Q}.$$

PROOF. – If Q is symmetric, then P is symmetric and the proposition is a consequence of Theorem 3.3.1. If Q is not symmetric, form the set

$$E = \{\varphi_\sigma(Q) \mid \sigma \in S_n\}.$$

The product $\prod_{q \in E} q$ is a symmetric polynomial of which Q is a factor. Because we have

$$\frac{P}{Q} = \frac{P \prod_{q \in E - \{Q\}} q}{\prod_{q \in E} q},$$

and we are again in the case where both numerator and denominator are symmetric. ◊

3.3.3 Proposition

Let P be a symmetric polynomial in n variables. If S is a polynomial of degree n having roots $a_1, \dots, a_n$, the numbers $P(a_1, \dots, a_n)$ belong to the ring generated by the coefficients of S.

PROOF. – This is an immediate and important consequence of Theorem 3.3.1 and Proposition 3.2.2. ♢

3.4 Newton's Formulas

PROPOSITION. – *For every integer $d \geq 1$, set*

$$p_d = \sum_{1 \leq i \leq n} (X_i)^d$$

in $A[X_1, \dots, X_n]$.

For $d \geq 1$, this gives

$$p_d = \sum_{1 \leq k \leq d-1} (-1)^{k-1} s_k p_{d-k} + (-1)^{d-1} d s_d.$$

EXAMPLES. –

$d = 1 : p_1 = s_1$;
$d = 2 : p_2 = s_1 p_1 - 2s_2$; for example $X^2 + Y^2 = (X+Y)(X+Y) - 2XY$;
$d = 3 : p_3 = s_1 p_2 - s_2 p_1 + 3s_3$; for example

$$X^3 + Y^3 + Z^3 = (X + Y + Z)(X^2 + Y^2 + Z^2) \\ -(XY + YZ + ZX)(X + Y + Z) + 3XYZ.$$

COMMENTARY. – This formula, which was stated by Newton around 1666 and published in 1707, makes it possible to successively compute the polynomials p_d given by the sums of the d-th powers of the X_i. Recall that $s_k = 0$ for $k > n$, which truncates the formula when $d > n$.

In 1629, Girard gave the expression of the p_d as a function of the s_k for $d \leq 4$ (Figure 3.2); in his charming terminology, the first "meslé" and second "meslé" are s_1, s_2. In his example, $X^4 + 35X^2 + 24 = 10X^3 + 50X$; the terms are placed on both sides of the equal sign in order to avoid negative signs. This is the first time that roots, including *impossible* ones, appear within formulas exactly like ordinary numbers.

Exemple.

Soit { A premier meſlé, B ſecond. C troiſieſme. D quatrieſme. &c.

alors en toute ſorte d'equation. { A ; A q — B 2 ; A cub — A B 3 + C 3 ; A q q — A q B 4 + A C 4 + B q 2 — D 4 } ſera la ſomme des { ſolutions ; quarez ; Cubes ; quaré-quarez }

Et pour mieux expliquer le tout, ſoit 1 (4) + 35 (2) + 24 eſgale à 10 (3) + 50 (1) : l'ordre des meſlez eſt 10. 35. 50. 24 pour A, B, C, D, cy-deſſus : tellement que 10 eſt voirement la ſomme des ſolutions qui ſont (1, 2, 3, 4.) Or A q — B 2, c'eſt à dire le quarré de 10 — deux fois 35 c'eſt la ſomme des quarrez, & ainſi du reſte ;

FIGURE 3.2. Excerpt from the book *Invention nouvelle...* by Girard, 1629

Setting $X = X_i$ in formula (3.1) from Proposition 3.2.2 gives

$$X_i^n = \sum_{1 \le k \le n} (-1)^k s_k X_i^{n-k}.$$

This gives the X_i^d for $d \ge n$ and the p_d by summation. It would remain to give a proof for $d < n$, which is possible.

The following method gives a proof valid for all $d \ge 0$, in the framework of the A-algebra $F = A[[X_1, \ldots, X_n]]$ of formal power series in n indeterminates with coefficients in A.

PROOF. – Consider the map $D : F \to F$ defined on the homogeneous parts of degree k of F by $D(u) = ku$, and more generally, for a formal power series $u = \sum_{k \ge 0} u_k$ written as the sum of its homogeneous parts of degree k, by $D(u) = \sum_{k \ge 0} k u_k$.

The operation D satisfies $D(u+v) = D(u) + D(v)$ and $D(uv) = D(u)v + uD(v)$. This D is an example of what we call a derivation in a ring; here,

$$D = \sum_{1 \le i \le n} X_i \frac{\partial}{\partial X_i}.$$

Indeed, if $u = \sum_{k \ge 0} u_k$ and $v = \sum_{k \ge 0} v_k$ are the expressions for u and v as sums of their homogeneous parts, we have

$$\begin{aligned}
D(uv) &= D\Big[\Big(\sum_{k\geq 0} u_k\Big)\Big(\sum_{k\geq 0} v_k\Big)\Big] \\
&= D\Big[\sum_{m\geq 0}\Big(\sum_{k+l=m} u_k v_l\Big)\Big] \\
&= \sum_{m\geq 0} m\Big(\sum_{k+l=m} u_k v_l\Big) \\
&= \sum_{m\geq 0}\sum_{k+l=m} (k u_k v_l + l u_k v_l) \\
&= \sum_{m\geq 0}\sum_{k+l=m} (k u_k) v_l + \sum_{m\geq 0}\sum_{k+l=m} u_k (l v_l) \\
&= D(u)v + uD(v).
\end{aligned}$$

It follows that the derivation of the product of r formal power series $u_1, \dots, u_r$ is given by

$$D(u_1 \cdots u_r) = D(u_1)(u_2 \cdots u_r) + \cdots + (u_1 \cdots u_{r-1})D(u_r);$$

so for invertible power series, we have

$$\frac{D(u_1 \dots u_r)}{u_1 \dots u_r} = \frac{D(u_1)}{u_1} + \cdots + \frac{D(u_r)}{u_r}.$$

Let us apply this formula to the n power series $u_i = 1 + X_i, 1 \leq i \leq n$, noting that $D(1+X_i) = X_i$. We obtain

$$\frac{D\Big(\prod_{1\leq i\leq n}(1+X_i)\Big)}{\prod_{1\leq i\leq n}(1+X_i)} = \frac{X_1}{1+X_1} + \cdots + \frac{X_r}{1+X_r}.$$

Recall that the inverse of $1 - X$ is the series $\sum_{k\geq 0} X^k$. Thus,

$$\frac{X}{1+X} = \sum_{k\geq 0}(-1)^k X^{k+1}.$$

Setting $X = -1$, formula (3.1) gives $\prod_{1\leq i\leq n}(1+X_i) = \sum_{0\leq k\leq n} s_k$, and since $s_k = 0$ for $k > n$, this gives $\prod_{1\leq i\leq n}(1+X_i) = \sum_{0\leq k} s_k$.

As $D\left(\sum_{0\leq k} s_k\right) = \sum_{1\leq k} k s_k$, we can now finish the proof:

$$\sum_{1\leq k} k s_k = D\Big(\sum_{0\leq k\leq n} s_k\Big) = D\Big[\prod_{1\leq i\leq n}(1+X_i)\Big]$$

$$= \left[\prod_{1\le i\le n}(1+X_i)\right]\left[\frac{X_1}{1+X_1}+\cdots+\frac{X_r}{1+X_r}\right]$$

$$= \left[\sum_{0\le k\le n} s_k\right]\sum_{1\le i\le n}\sum_{k\ge 0}(-1)^k(X_i)^{k+1}$$

$$= \left[\sum_{0\le k\le n} s_k\right]\sum_{k\ge 1}(-1)^{k-1}p_k$$

$$= \sum_{1\le d}\sum_{k+l=d}(-1)^{l-1}s_k p_l$$

$$= \sum_{1\le d}\left[(-1)^{d-1}p_d+\sum_{1\le k\le d-1}(-1)^{d-k-1}s_k p_{d-k}\right],$$

given that $s_0 = 1$. We conclude by identifying the homogeneous components of this last equality. ◇

3.5 Resultant of Two Polynomials

The resultant of two polynomials was introduced by Newton in certain special cases (1707), and then by Euler (1748, 1764) and by Bézout (1764).

3.5.1 Definition

Let K be a field contained in an algebraically closed field C (see §16.1). Let F and G be two polynomials in $K[X]$, of degree m and n respectively. Write

$$F(X) = a\prod_{1\le i\le m}(X-x_i) \quad\text{and}\quad G(X) = b\prod_{1\le i\le n}(X-y_i)$$

in $C[X]$.

The *resultant* of the two non-zero polynomials F and G is defined to be the product

$$\operatorname{Res}(F,G) = a^n b^m \prod_{1\le i\le m,1\le j\le n}(x_i-y_j).$$

If $F=0$ or $G=0$, we set $\operatorname{Res}(F,G)=0$.

REMARK. – The result is independent of the choice of C, as we will see. We will write $\operatorname{Res}_X(F,G)$ whenever it is necessary to distinguish the variable with respect to which the resultant is taken.

3.5.2 Proposition

1) *The resultant of two polynomials in $K[X]$ is zero if and only if the two polynomials have a common root in C.*

2) *The resultant of two polynomials in $K[X]$ is zero if and only if the two polynomials have a greatest common divisor which is neither a constant nor zero in $K[X]$.*

3) *The resultant of two non-zero polynomials in $K[X]$ is an element of K, and we have*

Formula (1): $$\operatorname{Res}(F,G) = a^n \prod_{1\le i\le m} G(x_i),$$

Formula (2): $$\operatorname{Res}(G,F) = (-1)^{mn}\operatorname{Res}(F,G),$$

Formula (3): $$\operatorname{Res}(F,G) = (-1)^{mn} b^{m-\deg(R)}\operatorname{Res}(G,R)$$

if the Euclidean division of F by G gives $F = GQ + R$ with $\deg(R) < \deg(G)$. *If $R = 0$, then* $\operatorname{Res}(F,G) = 0$.

Formula (4): $\operatorname{Res}(F,b) = b^m$ *for a constant polynomial b.*

PROOF. –

1) If F and G are non-zero and if $\operatorname{Res}(F,G) = 0$, then there exist i and j such that $x_i = y_j$. The converse is obvious.

2) Suppose that F and G are non-zero, as the result is obvious if one or both of them is zero. Because F and G have coefficients in K, we know that we can compute their greatest common divisor S in $K[X]$, and that S is also the greatest common divisor of F and G in C. If F and G have a common root x_i in C, then $X - x_i$ divides F and G, so it divides S; this means that S is not a constant. Conversely, if S is not a constant, then every root of S in C is a common root of F and G. Now part 1) suffices to conclude.

3) Formula (1):

$$\operatorname{Res}(F,G) = a^n \prod_{1\le i\le m}\left[b \prod_{1\le j\le n}(x_i - y_j)\right] = a^n \prod_{1\le i\le m} G(x_i).$$

Formula (2):

$$\prod_{1\le i\le m, 1\le j\le n}(x_i - y_j) = (-1)^{mn}\prod_{1\le i\le m, 1\le j\le n}(y_j - x_i).$$

Formula (3): formulas (1) and (2) give

$$\begin{aligned}\operatorname{Res}(F,G) &= (-1)^{mn}\operatorname{Res}(G,F)\\ &= (-1)^{mn}\operatorname{Res}(G, GQ+R)\end{aligned}$$

$$= (-1)^{mn} b^m \prod_{1 \le i \le n} [G(y_i)Q(y_i) + R(y_i)]$$
$$= (-1)^{mn} b^m \prod_{1 \le i \le m} R(y_i)$$
$$= (-1)^{mn} b^{m-\deg(R)} \mathrm{Res}(G, R).$$

Formula (4): this follows from formula (1).

The process of Euclidean division produces only elements of K, so the resultant $\mathrm{Res}(F, G)$ lies in K by definition. ◇

REMARKS. – Formulas (1)–(4) give an algorithm for computing the resultant.

Historically, the resultant was introduced as a determinant (see Exercise 3.3). This approach is very natural and actually renders the result of Proposition 3.5.2 c) more precise. Indeed, if

$$F(X) = \sum_{0 \le k \le m} a_k X^k \quad \text{and} \quad G(X) = \sum_{0 \le k \le n} b_k X^k,$$

then

$$\mathrm{Res}(F, G) \in A[a_0, \dots, a_m, b_0, \dots, b_n].$$

But to compute this determinant quickly, in general, one needs to revert to the method presented above.

3.6 Discriminant of a Polynomial

3.6.1 Definition

Let K be a field contained in an algebraically closed field C. The *discriminant* $D(P)$ of a non-zero polynomial P in $K[X]$ of degree n, with leading coefficient a, is defined by

$$D(P) = \frac{(-1)^{n(n-1)/2} \mathrm{Res}(P, P')}{a}.$$

3.6.2 Proposition

The discriminant $D(P)$ of a non-constant polynomial P is an element of K, which is equal to zero if and only if P is a root of multiplicity greater than or equal to 2 in C.

PROOF. – The fact that $D(P) \in K$ follows from Proposition 3.5.2 c). By Proposition 3.5.2 a), the discriminant of P, which is the resultant of P and P', is zero if and only if P has a common root with P' in C, i.e. if P has a root of multiplicity greater than or equal to 2 in C. ◇

3.6.3 Formulas

1) $D(aX^2 + bX + c) = b^2 - 4ac$.

2) $D(X^3 + pX + q) = -4p^3 - 27q^2$.

3) If $F(X) = a \prod_{1\leq i\leq n} (X - x_i)$, then $D(F) = a^{2n-2}\prod_{1\leq i<j\leq n}(x_i - x_j)^2$.

PROOF. – The proofs are contained in Exercise 3.5. ◇

3.6.4 Polynomials with Real Coefficients: Real Roots and Sign of the Discriminant

Second-degree polynomials

Let a, b, c be real numbers. We have $D(aX^2 + bX + c) = b^2 - 4ac = a^2(x_1 - x_2)^2$, where x_1 and x_2 denote the roots of $aX^2 + bX + c$ in $\mathbb{C}$. If x_1 and x_2 are distinct real numbers, we have $b^2 - 4ac > 0$. If they are not real, then they are conjugate in $\mathbb{C}$, $x_1 - x_2$ is a purely imaginary number, and $b^2 - 4ac < 0$.

Cubic polynomials

Let p, q be real numbers, and let a, b, c denote the roots of the polynomial X^3+ pX + q in $\mathbb{C}$. We have

$$D(X^3 + pX + q) = -4p^3 - 27q^2 = (a - b)^2(a - c)^2(b - c)^2.$$

If the three roots are distinct real numbers, then $-4p^3 - 27q^2 > 0$; this is the irreducible case (see §2.2.6). The second case is when two of the roots, say a and b, are not real numbers, but complex conjugates in $\mathbb{C}$; then $a - b$ is purely imaginary and its square is negative: $(a - c)^2$ and $(b - c)^2$ are conjugate and their product is strictly positive, so $-4p^3 - 27q^2 < 0$.

These results are summarized in Table 3.1.

	$D > 0$	$D < 0$
Degree 2	2 real roots	2 non-real conjugate roots
Degree 3	3 real roots	1 real root, 2 non-real conjugate roots

TABLE 3.1. Real roots and sign of the discriminant

Exercises for Chapter 3

Exercise 3.1. Elementary symmetric polynomials

1) Write the following symmetric polynomials as polynomials in the elementary symmetric polynomials:

   a) $X^2Y^2 + Y^2Z^2 + Z^2X^2$,

   b) $X^3Y + XY^3 + X^3Z + XZ^3 + Y^3Z + YZ^3$.

2) Use Newton's formulas to compute the sum of the fourth powers of the roots of the polynomial $(X-1)(X-2)(X-3)(X-4)$; check your result directly.

3) Compute the sum of the seventh powers of the roots of $X^3 + pX + q$.

4) Supposing that $q \neq 0$, determine the monic polynomial whose roots are the inverses of the squares of the roots of the polynomial $X^3 + pX + q$.

5) Let $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ be two n-tuples in K^n such that there exists no permutation σ in S_n such that $(y_{\sigma(1)}, \ldots, y_{\sigma(n)}) = (x_1, \ldots, x_n)$. Show that there exists an elementary symmetric polynomial s_k for some $1 \leq k \leq n$ such that $s_k(x_1, \ldots, x_n) \neq s_k(y_1, \ldots, y_n)$.

Exercise 3.2. Tschirnhaus' method

Consider the polynomials $P(X) = X^3 + pX + q$ with $pq \neq 0$ and $Q(X) = X^2 + a_1X + a_0$, where all coefficients lie in a subfield K of $\mathbb{C}$.

Suppose that P has a root x and set $y = Q(x)$.

The reader who quails before the rather lengthy computations involved in this exercise may employ the following shortcut: plug the results given in the solution to this exercise back into the exercise and check that they work.

1) Write the linear polynomial R which vanishes at x in terms of y and the coefficients of P and Q.

2) a) Compute $\text{Res}(P, Q - y)$.

   b) Determine elements a_0 and a_1 such that y satisfies a relation of the form $y^3 = a^3$.

3) Using the above, find the roots of P.

COMMENTARY. – In 1683, Tschirnhaus proposed his method for solving an equation of degree n by using a change of variables of the form $Y = Q(X)$, where Q is a polynomial of degree $n-1$, in order to reduce to an equation of the form $Y^n = a^n$ whose solutions are known; it then remains to solve the equation $Y = Q(X)$ which is of degree $n-1$. By induction, this method was supposed to give solutions of polynomial equations of all degrees. But it came to be understood later that the determination of the coefficients of Q led to equations of degree $> n$ unless $n = 2$ or 3, and that for $n = 4$, one obtains an equation of degree 6 which factors into two equations of degree 3.

Exercise 3.3. The resultant as a determinant

Let A be an integral domain. Consider the polynomials

$$\begin{aligned} F(X) &= a \prod_{1\le i\le m} (X - X_i) = \sum_{0\le k\le m} a_k X^k, \\ G(X) &= b \prod_{1\le i\le n} (X - Y_i) = \sum_{0\le k\le n} b_k X^k, \end{aligned}$$

in the ring $A[X_1, \ldots, X_m, Y_1, \ldots, Y_n]$. Let us define an $(m+n) \times (m+n)$ matrix $\Delta = (d_{jk})$ (here j and k denote the row and column indices respectively) with coefficients in $A[X_1, \ldots, X_m, Y_1, \ldots, Y_n]$, as in Figure 3.3.

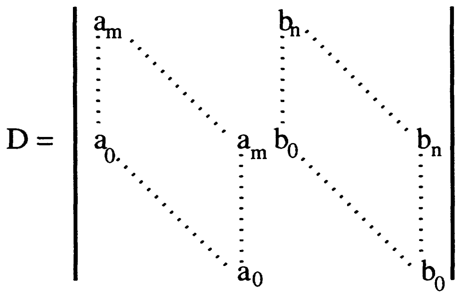


FIGURE 3.3. The matrix Δ

a) In the n first columns (i.e. $1 \le k \le n$), we set $d_{jk} = a_{m-j+k}$ for $k \le j \le k+m$, otherwise $d_{jk} = 0$.

b) In the m last columns (i.e. $n+1 \le k \le m+n$), we set $d_{j,k} = b_{k-j}$ for $k-n \le j \le k$, otherwise $d_{jk} = 0$.

Define D to be the determinant of the matrix Δ. Our goal is to check that $D = \operatorname{Res}(F, G)$ by the following steps.

1) Let N be an integer, and let $V(T_1, \ldots, T_N)$ denote the determinant (known as the Vandermonde determinant) of the square matrix $M(T_1, \ldots, T_N)$ of dimension n with coefficients in $\mathbb{Z}[T_1, \ldots, T_N]$ whose k-th row is given by $(T_k)^{N-1}, \ldots, (T_k)^2, T_k, 1$. Recall how to compute the Vandermonde determinant $V(T_1, \ldots, T_N)$.

2) Set $M = M(Y_1, \ldots, Y_n, X_1, \ldots, X_m)$. By computing the determinant $\det(M\Delta)$ in two different ways, show that $D = \mathrm{Res}(F, G)$.

3) Show that $\mathrm{Res}(F, G) \in A[a_0, \ldots, a_m, b_0, \ldots, b_n]$.

COMMENTARY. – In his memoir "A new way of eliminating unknown quantities from equations", presented to the Berlin Academy of Sciences in 1764, Euler introduced the resultant by writing that if two polynomials

$$F(X) = \sum_{0 \le k \le m} a_k X^k \quad \text{and} \quad G(X) = \sum_{0 \le k \le n} b_k X^k$$

have a common root x, then there exist polynomials

$$F_1(X) = \sum_{0 \le k \le m-1} x_k X^k \quad \text{and} \quad G_1(X) = \sum_{0 \le k \le n-1} y_k X^k$$

such that

$$F(X) = (X - x)F_1(X) \qquad \text{and} \qquad G(X) = (X - x)G_1(X).$$

Thus $FG_1 = F_1G$, and when this is expanded we obtain a system of linear equations in the x_i and y_j with $m+n$ equations and $m+n$ unknowns, whose determinant must be zero in order for there to exist a non-zero solution. This determinant is exactly the one which we introduced above; of course, Euler did not call it a determinant (this terminology was introduced by Sylvester in 1840), and he only wrote the explicit formula for polynomials of small degree.

Exercise 3.4. Computing the resultant

1) Let F, G_1 and G_2 be polynomials with coefficients in a field K. Check that $\mathrm{Res}(F, G_1G_2) = \mathrm{Res}(F, G_1)\mathrm{Res}(F, G_2)$.

2) Compute $\mathrm{Res}(aX^2 + bX + c, dX + e)$ in three different ways: using the formula using the roots of one of the polynomials, using the method of Euclidean division, and computing a determinant.

3) Show that

$$\begin{aligned}
&\mathrm{Res}(aX^2 + bX + c,\, a'X^2 + b'X + c') \\
&\qquad = \quad (a'c - ac')^2 - (ab' - a'b)(bc' - b'c) \\
&\qquad = \quad \left(ac' + a'c - \frac{bb'}{2}\right)^2 - \frac{1}{4}(b^2 - 4ac)(b'^2 - 4a'c').
\end{aligned}$$

Exercise 3.5. The discriminant of a polynomial

1) Compute $D(aX^2 + bX + c)$, $D(X^3 + pX + q)$.

2) Show that if $F(X) = a \prod_{1 \leq i \leq n} (X - x_i)$, then its discriminant satisfies

$$D(F) = a^{2n-2} \prod_{1 \leq i < j \leq n} (x_i - x_j)^2.$$

3) Show that $D(F)$ is real if F has real coefficients.

4) Let P be a polynomial with real coefficients and with roots that may or may not be real but which are pairwise distinct. What does the sign of $D(P)$ imply about the number of real roots of the equation $P(X) = 0$?

5) Let us give an application of the notion of discriminant which is beyond the actual scope of this book.

Equip the set E of polynomials of degree $\leq n$ in $\mathbb{C}[X]$ with the topology of $\mathbb{C}^{n+1}$ by identifying the element $(a_0, \ldots, a_n) \in \mathbb{C}^{n+1}$ with the polynomial $P = \sum_{0 \leq k \leq n} a_k X^k$.

a) Show that the polynomials having only simple roots form an open set of E.

b) Deduce from this that the $n \times n$ matrices with distinct eigenvalues form an open set of the set $M_n(\mathbb{C})$ of $n \times n$ matrices with entries in $\mathbb{C}$.

Exercise 3.6. Computating $D(X^{n-1} + X^{n-2} + \cdots + 1)$ for $n \geq 2$

1) Compute $D(X^n - 1)$ for $n \geq 1$.

2) Compute $D(X + 1), D(X^2 + X + 1), D(X^3 + X^2 + X + 1)$.

3) Show that if $P(X) = (X - x_1)P_1(X)$, then $D(P) = P_1(x_1)^2 D(P_1)$.

4) Compute $D(X^{n-1} + X^{n-2} + \cdots + 1)$ for $n \geq 2$.

5) Obtain the result of part **4)** by using the formulas

$$D(P) = \frac{(-1)^{n(n-1)/2}\mathrm{Res}(P, P')}{a} \quad \text{and} \quad \mathrm{Res(F, G)} = \mathrm{a^n} \prod_{1 \leq i \leq m} \mathrm{G(x_i)}.$$

Exercise 3.7. Descartes' Lemma

Let $n \geq 1$ be an integer, and let $(x_0, \ldots, x_n)$ be a family of real numbers.

We say that the family has a sign change at index i for $1 \leq i \leq n$ if and only if there exists $k \in \{0, \ldots, i-1\}$ such that $x_k x_i < 0$ and $x_l = 0$ for all l such that $k < l < i$.

If P is a polynomial in $\mathbb{R}[X]$, write $c(P)$ for the number of sign changes in the sequences of coefficients of P, and let $r(P)$ denote the number of strictly positive real roots of P.

1) Show that $r(P) \leq c(P)$ for every polynomial in $\mathbb{R}[X]$. To do this, reduce to the case where $P(0) \neq 0$ and use induction: if

$$P = \sum_{0 \leq k \leq n} a_k X^k$$

is a polynomial of degree n, set $k = \inf\{i \mid i > 0 \text{ and } a_i \neq 0\}$ and study the variations of P.

2) Give an upper bound for the number of strictly negative roots of P.

3) Determine the number of strictly positive roots, strictly negative roots, and non-real roots of the polynomial $X^8 + X^4 + X - 1$.

4) Let us study another situation. Let

$$P(X) = X^n + \sum_{k \leq n-p-1} a_k X^k$$

with $p \geq 0$ and $a_{n-p-1} \neq 0$, and write $s(P)$ for the number of real roots of P. Show that

- **a)** if p is even, then $s(P) \leq n - p$;
- **b)** if p is odd and $a_{n-p-1} > 0$, then $s(P) \leq n - p - 1$; and
- **c)** if p is odd and $a_{n-p-1} < 0$, then $s(P) \leq n - p + 1$.

COMMENTARY. – The subject of Exercise 3.7 is not directly related to the subject of this book; it was stated without proof by Descartes, and subsequently became the object of a great deal of discussion and many more or less incomplete proofs, until Gauss gave a complete proof in 1828. Any classical algebra text contains results of Sturm generalizing this lemma.

Solutions to Some of the Exercises

Solution to Exercise 3.1.

1) a) Set $P(X,Y,Z) = X^2Y^2 + Y^2Z^2 + Z^2X^2$. The polynomial P is symmetric in $\mathbb{Z}[X,Y,Z]$; its largest term for the ordering $X > Y > Z$ is X^2Y^2. So we compute $P - s_2^2$, i.e.

$$-2(X^2YZ + XY^2Z + XYZ^2) = -2s_1s_3.$$

This gives $P = s_2^2 - 2s_1s_3$.

b) See §3.3.

2) We have

$$(X-1)(X-2)(X-3)(X-4) = X^4 - 10X^3 + 35X^2 - 50X + 24,$$

and the sum $1^4 + 2^4 + 3^4 + 4^4 = 1 + 16 + 81 + 256 = 354$ confirms the computation

$$\begin{aligned} p_1 &= s_1 = 10, \\ p_2 &= s_1p_1 - 2s_2 = 30, \\ p_3 &= s_1p_2 - s_2p_1 + 3s_3 = 100, \\ p_4 &= s_1p_3 - s_2p_2 + s_3p_1 - 4s_4 = 354. \end{aligned}$$

3) Let x_1, x_2, x_3 denote the roots of $X^3 + pX + q$ in $\mathbb{C}$. By Euclidean division, we obtain

$$X^7 = (X^3 + pX + q)(X^4 - pX^2 - qX + p^2) + 2pqX^2 + (q^2 - p^3)X - p^2q,$$

which gives

$$\begin{aligned} \sum_{1\le i\le 3} (x_i)^7 &= \sum_{1\le i\le 3} [2pq(x_i)^2 + (q^2 - p^3)x_i - p^2q] \\ &= 2pqp_2 + (q^2 - p^3)s_1 - 3p^2q = -7p^2q, \end{aligned}$$

taking into account the identities $s_1 = 0$ and $p_2 = s_1p_1 - 2s_2 = -2p$. We can also successively compute the p_i: we find 0, $-2\,p$, $-3q$, $2p^2$, $5pq$, $-2p^3 + 3q^2$, $-7p^2q$.

4) Let a, b, c denote the roots of $X^3 + pX + q$ and S_1, S_2, S_3 the values of the elementary symmetric polynomials in $1/a^2$, $1/b^2$, $1/c^2$. Then

$$\begin{aligned} S_1 &= \frac{1}{a^2} + \frac{1}{b^2} + \frac{1}{c^2} = \frac{a^2b^2 + b^2c^2 + c^2a^2}{a^2b^2c^2} = \frac{p^2}{q^2}, \\ S_2 &= \frac{1}{a^2b^2} + \frac{1}{b^2c^2} + \frac{1}{c^2a^2} = \frac{a^2 + b^2 + c^2}{a^2b^2c^2} = -\frac{2p}{q^2}, \\ S_3 &= \frac{1}{q^2}. \end{aligned}$$

The desired polynomial is $X^3 - (p^2/q^2)X^2 - (2p/q^2)X - (1/q^2)$.

5) The polynomials $\prod_{1\le i\le n}(X - x_i)$ and $\prod_{1\le i\le n}(X - y_i)$ are distinct since they do not have the same roots; thus their coefficients are not all equal. The result follows from formula (3.1) in §3.2.2.

Solution to Exercise 3.2.

1) It suffices to divide $P(X)$ by $Q(X) - y$ via Euclidean division. We find the remainder $R(X) = (p - a_0 + a_1^2 + y)X + q + a_0a_1 - a_1y$.

2) a) The computation was begun in **1)**. We find that $\operatorname{Res}(P, Q - y)$ is equal to

$$-y^3 + (3a_0 - 2p)y^2 + (-3qa_1 - p(a_1)^2 - p^2 - 3(a_0)^2 + 4pa_0)y + C,$$

with $C = q^2 + 3qa_0a_1 - pqa_1 + p^2a_0 - 2p(a_0)^2 + (a_0)^3 - q(a_1)^3 + pa_0(a_1)^2$.

b) We see that $a_0 = (2p/3)$; we can then choose $a_1 = (3/p)\big(-(q/2)+A\big)$ with $A = \sqrt{(q^2/4) + (p^3/27)}$, so that $y^3 = (6A/p)^3\left(-(q/2) + A\right)$.

3) These choices give a polynomial R that is, up to a non-zero constant, of the form $X - B + (p/3B)$ where B is a cube root of $-(q/2) + A$, so what we have here are Cardan's formulas.

Solution to Exercise 3.3.

1) First, subtract from each column the following column multiplied by T_1, beginning with the first one. This gives

$$V(T_1, \ldots, T_N) = \prod_{2\le i\le N}(T_1 - T_i)V(T_2, \ldots, T_N).$$

By induction, we obtain

$$V(T_1, \ldots, T_N) = \prod_{1\le i<j\le N}(T_i - T_j).$$

2) Note that $F(Y_j) = \sum_{0\le k\le m} a_k(Y_j)^k$ for $1 \le j \le n$, $F(X_j) = 0$ for $1 \le j \le m$, $G(X_j) = \sum_{0\le k\le n} b_k(X_j)^k$ for $1 \le j \le m$, and $G(Y_j) = 0$ for $1 \le j \le n$.

Take the product $M\Delta$ and consider its determinant. For $1 \le j \le n$, $F(Y_j)$ is a factor throughout the j-th row; for $n + 1 \le j \le n + m$, $G(X_{j-n})$ is a factor throughout the j-th row. Once we have factored out these quantities, we are left with a determinant which can be computed as a product of the

determinants of two blocks, each of which is a Vandermonde determinant. We find

$$\det(M\Delta) = \prod_{1\le j\le m} F(Y_j) \prod_{1\le i\le n} G(X_i) V(X_1,\dots,X_m)V(Y_1,\dots,Y_n).$$

Comparing this with the product $\det(M)\det(\Delta)$, we find

$$\prod_{1\le j\le m} F(Y_j) \prod_{1\le i\le n} G(X_i) V(X_1,\dots,X_m)V(Y_1,\dots,Y_n)$$
$$= DV(Y_1,\dots,Y_n,X_1,\dots,X_m).$$

We have

$$V(Y_1,\dots,Y_n,X_1,\dots,X_m)$$
$$= V(X_1,\dots,X_m)V(Y_1,\dots,Y_n) \prod_{1\le i\le m, 1\le j\le n} (Y_j - X_i).$$

Consequently,

$$\prod_{1\le j\le n} F(Y_j) \prod_{1\le i\le m} G(X_i) = D \prod_{1\le i\le m, 1\le j\le n} (Y_j - X_i).$$

The result is then obtained by multiplying the two terms by a^n and simplifying by $\prod_{1\le j\le n} F(Y_j)$.

3) The computation of the determinant gives an element of the ring in the statement.

REMARK. – Here, in computing the determinant, we can make zeros appear simultaneously in the places of the coefficients of the highest degree terms in the columns corresponding to the highest degree polynomial, and then continue to repeat this procedure: it is exactly the algorithm of Euclidean division.

Solution to Exercise 3.4.

1) Use the formulas from the text.

2) a) The root of $dX + e$ is equal to $-e/d$, so we have

$$\operatorname{Res}(dX+e, aX^2+bX+c) = d^2\left(a\frac{e^2}{d^2} - b\frac{e}{d} + c\right) = cd^2 - bde + ae^2.$$

Furthermore, we have

$$aX^2+bX+c = (dX+e)\left(\frac{a}{d}X + \frac{db-ae}{d^2}\right) + \frac{cd^2-bde+ae^2}{d^2},$$

hence

$$\begin{aligned}\operatorname{Res}(aX^2+bX+c,dX+e) &= d^2\operatorname{Res}\left(dX+e,\frac{cd^2-bde+ae^2}{d^2}\right)\\ &= cd^2-bde+ae^2.\end{aligned}$$

The same result can be obtained by computing the determinant $\begin{vmatrix} a & d & 0\\ b & e & d\\ c & 0 & e\end{vmatrix}$.

3) We find

$$\begin{aligned}&\operatorname{Res}(aX^2+bX+c,a'X^2+b'X+c')\\ &= a\operatorname{Res}\left(aX^2+bX+c,\frac{ab'-a'b}{a}X+\frac{ac'-a'c}{a}\right)\\ &= a\left[c\left(\frac{ab-a'b}{a}\right)^2-b\left(\frac{ab'-a'b}{a}\right)\left(\frac{ac'-a'c}{a}\right)+a\left(\frac{ac'-a'c}{a}\right)^2\right]\\ &= (a'c-ac')^2-(ab'-a'b)(bc'-b'c).\end{aligned}$$

The second formula is obtained by a simple computation.

Solution to Exercise 3.5.

1) It is possible to use several different formulas to compute the resultant. For example, if x_1 and x_2 are the roots of aX^2+bX+c in $\mathbb{C}$, we have

$$\begin{aligned}D(aX^2+bX+c) &= -(2ax_1+b)(2ax_2+b)\\ &= -4a^2\left(\frac{c}{a}\right)-2ab\left(-\frac{b}{a}\right)-b^2\\ &= b^2-4ac.\end{aligned}$$

Similarly, because $\sqrt{(-p/3)}$, $-\sqrt{(-p/3)}$ are the roots of $3X^2+p$, we have

$$\begin{aligned}&D(X^3+pX+q) = -\operatorname{Res}(X^3+pX+q,3X^2+p)\\ &= -27\left[\left(\sqrt{\frac{-p}{3}}\right)^3+p\sqrt{\frac{-p}{3}}+q\right]\left[-\left(\sqrt{\frac{-p}{3}}\right)^3-p\sqrt{\frac{-p}{3}}+q\right]\\ &= -27\left[\frac{2p}{3}\sqrt{\frac{-p}{3}}+q\right]\left[-\frac{2p}{3}\sqrt{\frac{-p}{3}}+q\right] = -4p^3-27q^2.\end{aligned}$$

Now, if a, b, c denote the roots of X^3+pX+q in $\mathbb{C}$, then using a formula from Exercise 3.1, we obtain

$$D(X^3+pX+q) \quad = \quad -(3a^2+p)(3b^2+p)(3c^2+p)$$

$$\begin{aligned}
&= -27a^2b^2c^2 - 9p(a^2b^2 + b^2c^2 + \\
&\qquad c^2a^2) - 3p(a^2 + b^2 + c^2) - p^3 \\
&= -27q^2 - 9p[(ab + bc + ca)^2 - (a + b + c)abc] \\
&\qquad -3p^2[(a + b + c)^2 - 2(ab + bc + ca)] - p^3 \\
&= -27q^2 - 9p[p^2] - 3p^2[-2p] - p^3 \\
&= -4p^3 - 27q^2.
\end{aligned}$$

These computations can also be done using the method of Euclidean division or by computing a determinant.

2) Taking into account the $(n^2 - n)/2$ sign changes to be made in the product, we have

$$\begin{aligned}
D(F) &= \frac{(-1)^{n(n-1)/2}\mathrm{Res}(F, F')}{a} \\
&= \frac{(-1)^{n(n-1)/2}a^{n-1} \prod_{1\leq i\leq n} F'(x_i)}{a} \\
&= (-1)^{n(n-1)/2}a^{n-2} \prod_{1\leq i\leq n} \left(a \prod_{1\leq j\leq n, j\neq i} (x_i - x_j) \right) \\
&= a^{2n-2} \prod_{1\leq i\leq j\leq n} (x_i - x_j)^2.
\end{aligned}$$

3) We know that the resultant belongs to the field generated by the coefficients of the polynomials.

4) If P has only real roots, then of course we have $D(P) > 0$.

If P does not have only real roots, then it has an even number of non-real roots, say k pairs of complex conjugates. Let us reason by regrouping the factors occurring in the formula of part **2)**.

For every non-real root x and every real root y, the terms $x - y$ and $\overline{x} - y$ are conjugate, so $(x - y)^2 \left(\overline{x} - y\right)^2 > 0$.

For every non-real root x and every non-real root y, the terms $x - y$ and $\overline{x} - \overline{y}$ are conjugate, as are the terms $\overline{x} - y$ and $x - \overline{y}$, so we have

$$(x - y)^2 \left(\overline{x} - \overline{y}\right)^2 \left(\overline{x} - y\right)^2 (x - \overline{y})^2 > 0.$$

For every non-real root x of P, we have $(x - \overline{x})^2 < 0$.

Thus, $D(P)$ has the same sign as $(-1)^k$. The final conclusion is that if $D(P) > 0$, $2k = 0 \bmod 4$ and if $D(P) < 0$, then $2k = 2 \bmod 4$.

5) a) The map which associates $D(P)$ to P is continuous (take the determinant to be the expression of the discriminant), and the set of

polynomials having only simple roots corresponds to the complement of the inverse image of 0, so it is open.

b) An $n\times n$ matrix has distinct eigenvalues if and only if its characteristic polynomial has no double roots. The rest follows immediately.

Solution to Exercise 3.6.

1) Applying the formulas for computing resultants, and using the fact that $(-1)^{n(n-1)} = 1$, we find

$$\begin{aligned} D(X^n-1) &= (-1)^{n(n-1)/2}\mathrm{Res}(X^n-1, nX^{n-1}) \\ &= (-1)^{n(n-1)/2}\mathrm{Res}(nX^{n-1}, X^n-1) \\ &= (-1)^{n(n-1)/2}n^n(-1)^{n-1}. \end{aligned}$$

Finally, $D(X^n-1) = (-1)^{(n-1)(n+2)/2}n^n$. In other words, we have

$$\begin{aligned} D(X^n-1) &= n^n \quad \text{if} \quad n = 1, 2 \bmod 4, \\ D(X^n-1) &= -n^n \quad \text{if} \quad n = 0, 3 \bmod 4. \end{aligned}$$

2) Using the formula $D(F) = a^{2n-2} \prod_{1\le i<j\le n} (x_i - x_j)^2$, we find

$$\begin{aligned} D(X+1) &= 1 \qquad \text{(empty product)}, \\ D(X^2+X+1) &= (j-j^2)^2 = -3, \\ D(X^3+X^2+X+1) &= [(i+1)2i(-1+i)]^2 = -16. \end{aligned}$$

3) If $P(X) = a \prod_{1\le i\le n} (X - x_i) = (X - x_1)P_1(X)$, we have

$$\begin{aligned} D(P) &= a^{2n-2} \prod_{1\le i<j\le n} (x_i - x_j)^2 \\ &= a^2 \prod_{1<i\le n} (x_1 - x_i)^2 a^{2n-4} \prod_{2\le i<j\le n} (x_i - x_j)^2 \\ &= P_1(x_1)^2 D(P_1). \end{aligned}$$

4) We have

$$\begin{aligned} (-1)^{(n-1)(n+2)/2}n^n &= D(X^n-1) \\ &= D[(X-1)(X^{n-1}+X^{n-2}+\cdots+1)] \\ &= n^2 D(X^{n-1}+X^{n-2}+\cdots+1), \end{aligned}$$

which gives

$$D(X^{n-1}+X^{n-2}+\cdots+1)=(-1)^{(n-1)(n+2)/2}n^{n-2}.$$

5) Set $P(X)=X^{n-1}+X^{n-2}+\cdots+1$. If $\zeta=e^{2i\pi/n}$, we have

$$D(P)=(-1)^{n(n-1)/2}\mathrm{Res}(P,P')=(-1)^{n(n-1)/2}\prod_{1\leq i\leq n-1}P'(\zeta^i).$$

As

$$P(X)=\frac{X^n-1}{X-1},$$

we have

$$P'(\zeta^i)=\frac{n\zeta^{(n-1)i}}{\zeta^i-1},$$

and because

$$\prod_{1\leq i\leq n-1}(\zeta^i-1)=(-1)^{n-1}P(1)=(-1)^{n-1}n,$$

we find the preceding result.

4
Field Extensions

In this chapter, we come to the basic notions of Galois theory. Abel and Galois defined the elements of a generated extension, but they did not envision these elements as forming a set. The concept of a field (and the word) did not appear until the work of Dedekind between 1857 and 1871. The abstract definition of a field was given about 20 years later by Weber and Moore. One hundred years ago, the language of linear algebra did not exist and results were formulated very differently from the way they are today, as can be seen, for example, in Weber's book, listed in the bibliography.

4.1 Field Extensions

4.1.1 Definition

An *extension of a field* K is a field containing K as a subfield. If M is an extension of K, then an intermediate extension (between K and M) is an extension L of K contained in M. We will usually represent field extensions in one of the forms shown in Figure 4.1, where the *upper* field is an extension of the *lower* field.

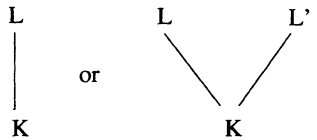


FIGURE 4.1.

More generally, an extension of a field K is a pair (L, i) where L is a field and $i : K \to L$ a ring homomorphism between two fields; such a homomorphism is necessarily injective (if $x \neq 0$, then x has an inverse x^{-1} and $i(x)i(x^{-1}) = i(xx^{-1}) = i(1) = 1$ shows that $i(x) \neq 0$).

4.1.2 Proposition

An extension L of a field K is naturally endowed with the structure of a K-vector space and even that of a K-algebra.

PROOF. – The K-algebra structure is defined by the addition and multiplication operations of L, and the K-action is simply the restriction of this multiplication to $K \times L$. ◇

4.1.3 The Degree of an Extension

Let L be an extension of a field K. The dimension of L as a K-vector space is called the degree of the extension L over K; it is written $[L : K]$. A field L is said to be a finite degree of K if $[L : K]$ is finite. An extension of degree 2 is called a quadratic extension.

COMMENTARY. – The rest of this book is devoted to the study of finite degree extensions, with just a few exceptions. The general study of extensions of infinite degree needs topology.

EXAMPLES. –

1) The fields $\mathbb{R}$ and $\mathbb{C}$ are not countable, so they are extensions of $\mathbb{Q}$ of infinite degree.

2) $\mathbb{R}(X)$ is an extension of infinite degree of $\mathbb{R}$.

3) $\mathbb{C}$ is a quadratic extension of $\mathbb{R}$, with basis $\{1, i\}$ for example.

4) $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2}; a, b \in \mathbb{Q}\right\}$ is a quadratic extension of $\mathbb{Q}$, with basis $\left\{1, \sqrt{2}\right\}$ for example.

4.1.4 Towers of Fields

In certain problems, for example the solvability by radicals considered in Chapter 12, one considers finite sequences of successive extensions $K = K_0 \subset \cdots \subset K_r$; such a sequence is called a tower of fields.

4.2 The Tower Rule

4.2.1 Proposition

Let L be a finite-degree extension of a field K, and let M be a finite-degree extension of L. Then M is a finite-degree extension of K, and we have

$$[M : K] = [M : L][L : K].$$

EXAMPLE. –

$$\left[\mathbb{Q}[\sqrt[3]{2}, j] : \mathbb{Q}\right] = \left[\mathbb{Q}[\sqrt[3]{2}, j] : \mathbb{Q}[\sqrt[3]{2}]\right] \left[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}\right] = 2 \cdot 3 = 6.$$

The fields in this example will be described more precisely after this chapter; they are algebraic extensions of $\mathbb{Q}$. The formula gives the degree of $\mathbb{Q}[\sqrt[3]{2}, j]$ over $\mathbb{Q}$, using the intermediate extension $\mathbb{Q}[\sqrt[3]{2}]$ and Proposition 4.5.2 below; we can also use the intermediate extension $\mathbb{Q}[j]$.

REMARK. – The above formula is also useful in the form "$[L : K]$ divides $[M : K]$."

PROOF. – Set $n = [L : K]$ and $p = [M : L]$, and let $\{l_1, \ldots, l_n\}$ denote a basis of L over K and $\{m_1, \ldots, m_p\}$ a basis of M over L. The np numbers $l_i m_j$ for $1 \le i \le n, 1 \le j \le p$, form a basis of M over K. Indeed,

1) They form a linearly independent system because if

$$\sum_{1 \le i \le n, 1 \le j \le p} x_{ij} l_i m_j = 0,$$

then

$$\sum_{1 \le j \le p} \Big(\sum_{1 \le i \le n} x_{ij} l_i \Big) m_j = 0.$$

But the m_j are linearly independent in the L-vector space M, so for $j = 1, \ldots, p$, we must have

$$\sum_{1 \le i \le n} x_{ij} l_i = 0.$$

Thus all the x_{ij} are zero because the l_i are linearly independent in the K-vector space L.

2) They form a generating system because if x is in M, then there exist $x_1, \ldots, x_p$ in L such that

$$x = \sum_{1 \le j \le p} x_j m_j,$$

and for each of the x_j there exist $x_{1j}, \dots, x_{nj}$ in K such that

$$x_j = \sum_{1 \le i \le n} x_{ij} l_j,$$

so

$$x = \sum_{1 \le j \le p} \Big(\sum_{1 \le i \le n} x_{ij} l_i \Big) m_j = \sum_{1 \le i \le n, 1 \le j \le p} x_{ij} l_i m_j.$$

◇

COROLLARY. – *Let M be a finite-degree extension of a field K and L an intermediate extension. Then L is a finite-degree extension of K and M is a finite-degree extension of L.*

PROOF. – If $\{l_1, \dots, l_n\}$ are elements of L that are linearly independent over K, and if $\{m_1, \dots, m_p\}$ are elements of M that are linearly independent over L, then by Proposition 4.2.1, the np numbers $l_i m_j$ for $1 \le i \le n, 1 \le j \le p$, are linearly independent over K. Thus $np \le [M : K]$, which bounds n and p. ◇

4.3 Generated Extensions

4.3.1 Proposition

Let L be an extension of a field K, and let A be a subset of L.

1) *There exists an extension of K, denoted by $K(A)$, which contains A and has the property that it is minimal, i.e. it is contained in every extension of K contained in L and containing A.*

2) *As a set, $K(A)$ is equal to the set E of elements of L of the form $S(a_1, \dots, a_k)/T(a_1, \dots, a_k)$, where k is an integer running through $\mathbb{N}$, $a_1, \dots, a_k$ are elements of A and S/T is a rational function in $K(X_1, \dots, X_k)$ of rational functions, such that $T(a_1, \dots, a_k) \neq 0$.*

PROOF. –

1) Consider the family of extensions of K contained in L and containing A. This family is non-empty since L belongs to it, and the intersection of all fields in the family satisfies the defining property of $K(A)$.

2) It is easy to see that every element of E lies in every extension of K contained in L and containing A. Furthermore, E is obviously a field containing K and A, so we obtain $E = K(A)$.

◇

4.3.2 Definition

The extension $K(A)$ is called the *extension of K generated by A*. If $A = \{a_1, \ldots, a_n\}$, then the extension $K(A)$ is usually written $K(a_1, \ldots, a_n)$.

4.3.3 Proposition

Let L be an extension of a field K, and let A, B be two subsets of L. Then

$$K(A \cup B) = K(A)(B).$$

PROOF. – By Proposition 4.3.1 1), we know the following facts.

- Because $A \cup B \subset K(A) \cup B \subset K(A)(B)$, we have $K(A \cup B) \subset K(A)(B)$.
- Because $K(A) \cup B \subset K(A \cup B)$, we have $K(A)(B) \subset K(A \cup B)$. ◇

4.4 Algebraic Elements

4.4.1 Definition

Let K be a field and L an arbitrary extension of K. An element a of L is said to be *algebraic over K* if there exists a non-zero polynomial in $K[X]$ having a as a root.

EXAMPLES. – $\sqrt{2}$, $\sqrt[3]{2}$, and $e^{2i\pi/n}$ are all complex numbers that are algebraic over $\mathbb{Q}$.

REMARK. – It is not obvious that the sum and product of two algebraic numbers over K is also algebraic; this is proved in §6.3.

4.4.2 Transcendental Numbers

A number that is not algebraic over K is called *transcendental over K*. A complex number transcendental over $\mathbb{Q}$ (such a number is simply called a transcendental number) is thus a number that is not a root of any polynomial with coefficients in $\mathbb{Z}$.

Joseph Liouville was the first to prove, in 1844, that certain real numbers are transcendental over $\mathbb{Q}$, for instance $\sum_{n>0} 10^{-n!}$ (see Exercise 4.1). Hermite proved the transcendence of e in 1873 (see Exercise 4.2), and Carl Lindemann proved the transcendence of π in 1882, finally providing a negative answer to the ancient problem of squaring the circle (i.e. using only ruler and compass to construct a square having area equal to that of a given circle).

Alexandre Gelfond and Theodor Schneider showed in 1934 that a^b is transcendental whenever a is algebraic, $a \neq 0$ and $a \neq 1$, and b is an irrational algebraic number. For example, $2^{\sqrt{2}}$ is transcendental. Alan Baker, a 1970 Fields Medalist, extended these results considerably at the end of the 1960s. It is still not known if numbers such as $e + \pi$ are transcendental or not. Transcendental number theory is at present a rapidly developing subject.

4.4.3 Minimal Polynomial of an Algebraic Element

PROPOSITION. – *Let K be a field, L an extension of K and a an element of L which is algebraic over K. There exists a unique monic polynomial P in $K[X]$ having a as a root and of minimal degree among all the non-zero polynomials in $K[X]$ having a as a root.*

PROOF. – Let us first show that the ring $K[X]$ is a principal ideal domain, i.e. every ideal of $K[X]$ is generated by a single element. This is true for the ideal $I = (0)$, and if I is a non-zero ideal of $K[X]$, then it contains a polynomial $P \neq 0$ of minimal degree, such that every other polynomial S of I is a multiple of P. Indeed, the Euclidean division of S by P gives an equality $S = PQ + R$ where the degree of R is strictly less than that of P, but $R = S - PQ$ is an element of I, contradicting minimality of the degree of P unless $R = 0$.

Now, consider the set I of polynomials of $K[X]$ which vanish at a. This forms a non-zero ideal of $K[X]$, so there exists a polynomial T of $K[X]$ such that $I = (T)$. Dividing T by its leading coefficient, we obtain a monic polynomial P which generates I.

The uniqueness of P is a consequence of the fact that if T is a monic polynomial in $K[X]$ satisfying the same conditions as P, then $P - T$ is an element of I which vanishes at a, so because its degree is $< \deg(P)$, it must be zero. ◇

4.4.4 Definition

Let K be a field and L an extension of K; let a be an element of L algebraic over K. By the preceding section, there exists a unique monic polynomial *of minimal degree* in $K[X]$ which vanishes at a; it is called the *minimal polynomial* of a over K. If $\deg(P) = n$, then a is said to be algebraic of degree n over K; we also say that n is the degree of a over K.

EXAMPLE. – $X^2 - 2$ is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$; $\sqrt{2}$ is of degree 2 over $\mathbb{Q}$.

REMARKS. – The minimal polynomial of an element a of K is $X - a$.

The minimal polynomial depends on the field K; thus $\sqrt[6]{2}$ has minimal polynomial $X^6 - 2$ over $\mathbb{Q}$, but $X^3 - \sqrt{2}$ over $\mathbb{Q}[\sqrt{2}]$.

4.4.5 Properties of the Minimal Polynomial

PROPOSITION. – *Let K be a field, L an extension of K and a an element of L which is algebraic over K of minimal polynomial P over K.*

1) *Every polynomial of $K[X]$ which vanishes at a is divisible by P.*

2) *P is irreducible over K, i.e. it is not the product of two non-constant polynomials in $K[X]$.*

3) *Every root of P lying in L has minimal polynomial P.*

4) *If L is a field of characteristic 0, in particular if $L \subset \mathbb{C}$, a is a simple root of P (we will say that P is separable; for a counterexample in an infinite field of non-zero characteristic, see §15.2).*

PROOF. –

1) This is an immediate consequence of the preceding proof.

2) If $P = ST \in K[X]$, the equality $P(a) = 0$ implies that $S(a) = 0$ or $T(a) = 0$. If neither S nor T is a constant, then $\deg(S) < \deg(P)$ and $\deg(T) < \deg(P)$, which is impossible.

3) Let b be a root of P in L; thus b is an algebraic number over K and so it has a minimal polynomial S over K. As $P(b) = 0$, P is a multiple of S by part 1), but as P is irreducible, this means that $P = S$.

4) Suppose that a is a root of order $k > 1$ of P, i.e. $P(X) = (X-a)^k S(X)$ in $\mathbb{C}[X]$, with $S(a) \neq 0$.
   We have $P'(X) = k(X-a)^{k-1}S(X)+(X-a)^k S'(X)$, so $P'(a) = 0$, which contradicts the definition of P as the minimal polynomial of a since $\deg(P') = \deg(P) - 1$ and P' is non-zero in $K[X]$.

◇

4.4.6 Proving the Irreducibility of a Polynomial in $\mathbf{Z}[X]$

An algorithm for factoring polynomials in $\mathbb{Z}[X]$ or in $(\mathbb{Z}/p\mathbb{Z})[X]$ into irreducible factors, developed by Berlekamp (1967), is now available as part of computer packages in formal computation. We discuss methods for factoring by hand. Let us first recall a classical result.

PROPOSITION. – *A polynomial in $\mathbb{Z}[X]$, whose content, which is the greatest common divisor of its coefficients, is equal to 1, is irreducible in $\mathbb{Q}[X]$ if and only if it is irreducible in $\mathbb{Z}[X]$.*

Thus, the irreducibility of a given polynomial in $\mathbb{Q}[X]$ can always be expressed as the irreducibility of a polynomial in $\mathbb{Z}[X]$, and it is enough to consider methods over $\mathbb{Z}$.

METHODS. – Let us now recall different practical methods for studying the irreducibility of a polynomial $P(X) = \sum_{0 \le k \le n} a_k X^k$ in $\mathbb{Z}[X]$ by hand.

1) *Eisenstein's criterion* proves that a polynomial P in $\mathbb{Q}[X]$ is irreducible if it satisfies the following condition: there exists a prime number p which does not divide a_n but divides all the other coefficients of P, whereas p^2 does not divide a_0. Sometimes, when the Eisenstein criterion is not directly applicable to a polynomial $P(X)$, it is applicable to $P(X + a)$ for some value of a.

   This criterion remains valid if we replace $\mathbb{Z}$ by any factorial ring A and the field $\mathbb{Q}$ by the fraction field of A, and if we assume the existence of a prime (i.e. irreducible) element p in A satisfying the above conditions.

2) To see if P does not have a rational root, assume that p/q is a rational root of P, written as a totally reduced fraction. Then $q^n P(p/q)$ is an integer, but it is equal to zero, so it follows that q divides a_n and p divides a_0, which makes it possible to obtain the set of rational candidates for roots of P. If this set does not have too many elements, we can test the candidates one by one.

3) If P is of degree 3 and has no rational root, then it is irreducible.

4) If P is of degree 4, has no rational root and is not decomposable as a product of two quadratic factors (to see this, one can use a method of indeterminate coefficients as in Exercise 2.7), then it is irreducible.

5) It is often useful to consider the reduction of a polynomial in $\mathbb{Z}[X]$ to the ring $(\mathbb{Z}/p\mathbb{Z})[X]$.

Indeed, if there exists a prime number p such that the image of P in $(\mathbb{Z}/p\mathbb{Z})[X]$ is an irreducible polynomial of the same degree, then P is itself irreducible (assuming that its content is equal to 1). The converse is false; the classical example is the polynomial $X^4 + 1$. We show later (in Exercise 14.8) that this polynomial is reducible modulo p for all primes p, although it is clearly irreducible in $\mathbb{Z}[X]$.

If the image of P in $(\mathbb{Z}/p\mathbb{Z})[X]$ is a polynomial of strictly smaller degree, we cannot conclude anything; for example, one can consider the polynomial $(pX + 1)(X + 1)$.

The irreducibility of P in $(\mathbb{Z}/p\mathbb{Z})[X]$ can be proved, for example:

1) for polynomials of degree 2 or 3, by systematically testing if the elements of $\mathbb{Z}/p\mathbb{Z}$ are roots of P;

2) for polynomials of degree 4, by systematically testing if the elements of $\mathbb{Z}/p\mathbb{Z}$ are roots of P and showing that a decomposition into a product of two quadratic polynomials is impossible;

3) for polynomials of degree n, by listing the irreducible polynomials of degree $\leq n/2$ and testing if they divide P.

Note, finally, that it is sometimes interesting to compare the degrees of the irreducible factors of the images of P in $(\mathbb{Z}/p\mathbb{Z})[X]$ and $(\mathbb{Z}/q\mathbb{Z})[X]$.

4.5 Algebraic Extensions

4.5.1 Extensions Generated by an Algebraic Element

Let L be an extension of a field K, and let a be an element of L which is algebraic over K. Let $K[a]$ denote the smallest subring containing K and a, i.e. the image of the homomorphism $f : K[X] \to L$ defined by $f(X) = a$, where $f|K$ denotes the inclusion of K into L.

Thus, the expressions $K[a]$ and $K(a)$ refer respectively to images of the ring of polynomials $K[X]$ and of the field of rational functions $K(X)$. If a is algebraic over K, these two images coincide.

4.5.2 Properties of $K[a]$

PROPOSITION. – *Let L be an extension of a field K, and let a be an element of L which is algebraic of degree n over K, with minimal polynomial P over K. Then*

1) $K[a]$ is an extension of K and $K[a] = K(a)$,

2) $[K[a] : K] = n$ and the set $\{a^k;\ 0 \leq k \leq n-1\}$ forms a basis of $K[a]$ as a K-vector space, and

3) The homomorphism $f : K[X] \to K[a]$ defined by $f(X) = a$ and $f(k) = k \in K[a]$ for $k \in K$ induces a K-algebra isomorphism $\varphi : K[X]/(P) \to K[a]$ which leaves the elements of K invariant and makes the diagram in Figure 4.2 commute (π denotes the canonical projection).

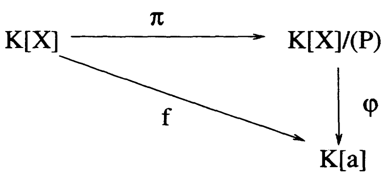


FIGURE 4.2.

PROOF. –

1) We have $K[a] \subset K(a)$, so let us show the inverse inclusion. By Proposition 4.3.1, every element of $K(a)$ is of the form $S(a)/T(a)$ with S and T in $K[X]$ and $T(a) \neq 0$; thus T is not divisible by P, and as P is irreducible over K, T is relatively prime to P. Bézout's theorem ensures the existence of polynomials U and V of $K[X]$ such that $UT + VP = 1$, which proves that $S(a)/T(a) = S(a)U(a)$. Thus $S(a)/T(a)$ belongs to $K[a]$.

2) Let us first show that the family $\{a^k; 0 \leq k \leq n-1\}$ is free over K. If there exists a family $\{\lambda_k; 0 \leq k \leq n-1\}$ of elements of K such that $\sum_{0 \leq k \leq n-1} \lambda_k a^k = 0$, the polynomial $S(X) = \sum_{0 \leq k \leq n-1} \lambda_k X^k$ in $K[X]$ vanishes at a. As $\deg(S) < \deg(P)$, we have $S = 0$, which proves that $\lambda_k = 0$ for $0 \leq k \leq n-1$.

   The family $\{a^k; 0 \leq k \leq n-1\}$ generates $K[a]$, because if S is a polynomial of $K[X]$ and if $S = PQ + R$ by Euclidean division, we have $S(a) = R(a)$. As $\deg(R) \leq n-1$, $R(a)$ belongs to the K-space generated by $\{a^k; 0 \leq k \leq n-1\}$.

3) The map f defined above has image $K[a]$, and kernel the set of polynomials vanishing at a, i.e. the ideal (P). This gives the desired factorization. ◊

4.5.3 Definition

An extension L of a field K is said to be *algebraic* if every element of L is algebraic over K.

EXAMPLE. – $\mathbb{C}$ is an algebraic extension of $\mathbb{R}$, because any complex number $a + ib$ with a and b real is a root of the polynomial $X^2 - 2aX + a^2 + b^2 = 0$ in $\mathbb{R}[X]$.

4.5.4 Extensions of Finite Degree

PROPOSITION. – *Let K be a field. Every extension L of K of finite degree n is algebraic over K, and every element of L is algebraic of degree $\leq n$ over K.*

PROOF. – Let $x \in L$. The family $\{x^k; 0 \leq k \leq n\}$ has more than n elements, so it is not linearly independent over K. This means that there exists a family $\{\lambda_k; 0 \leq k \leq n\}$ of elements of K, not all zero, such that $\sum_{0 \leq k \leq n-1} \lambda_k x^k = 0$. In other words, the polynomial $S(X) = \sum_{0 \leq k \leq n} \lambda_k X^k$ of $K[X]$ vanishes at x. Because $S \neq 0$, x is algebraic of degree $\leq n$ over K. ◊

4.5.5 Corollary: Towers of Algebraic Extensions

Let K be a field, and L an extension of K. Let r be an integer and $(K_i)_{0\leq i\leq r}$ a tower of extensions of K contained in L such that $K_0 = K$ and there exist elements $a_1, \ldots, a_r$ of L such that for $i = 1, \ldots, r$, a_i is algebraic of degree n_i over K_{i-1} and $K_i = K_{i-1}[a_i]$. Then K_r is an algebraic extension of K of degree $n = n_1 \ldots n_r$.

PROOF. – By §4.5.2, K_i is of degree n_i over K_{i-1}; the tower rule shows that K_n is an extension of finite degree n of K. Proposition 3.5.4 concludes the proof. ◇

4.6 Algebraic Extensions Generated by n Elements

4.6.1 Notation

Let L be an extension of a field K, and let $a_1, \ldots, a_n$ be elements of L which are algebraic over K. Write $K[a_1, \ldots, a_n]$ for the image of the homomorphism $f : K[X_1, \ldots, X_n] \to L$ defined by $f(P) = P(a_1, \ldots, a_n)$. It is the K-algebra generated by $a_1, \ldots, a_n$.

4.6.2 Proposition

With notation as above, $K[a_1, \ldots, a_n]$ is an algebraic extension of finite degree of K, equal to $K(a_1, \ldots, a_n)$.

PROOF. – By induction, we will construct the tower of extensions $(K_i)_{0\leq i\leq n}$ of K contained in L such that $K_0 = K$, and such that for each $i = 1, \ldots, n$, there exists an element a_i, algebraic over K (so also over K_{i-1}), such that $K_i = K_{i-1}[a_i]$. Corollary 4.5.5 shows that K_n is an algebraic extension of finite degree of K.

Let us show by induction on i that $K_i = K[a_1, \ldots, a_i]$ for $i = 1, \ldots, n$. The case $n = 1$ was considered in §4.5.2. Suppose that

$$K_{i-1} = K[a_1, \ldots, a_{i-1}].$$

Because every polynomial $P(X_1, \ldots, X_i)$ in $K[X_1, \ldots, X_i]$ can be written in the form $\sum_k P_k(X_1, \ldots, X_{i-1})(X_i)^k$, we have

$$P(a_1, \ldots, a_i) = \sum_k P_k(a_1, \ldots, a_{i-1})(a_i)^k,$$

so $K[a_1, \ldots, a_i] = K[a_1, \ldots, a_{i-1}][a_i] = K_{i-1}[a_i] = K_i$. As K_i is a field, we have $K_i = K(a_1, \ldots, a_i)$ for $i = 1, \ldots, n$. ◇

REMARK. – The degree of $K[a_1, \ldots, a_n]$ over K is less than or equal to the product of the degrees of the a_k over K.

4.6.3 Corollary

Let L be an extension of a field K and let a, b be elements of L that are algebraic over K. Then $a+b$, ab, a/b are all algebraic over K.

PROOF. – These elements belong to $K[a,b]$, which is an algebraic extension of finite degree of K by §4.6.2. ◇

COMMENTARY. – This corollary settles the point raised in §4.4.1: it proves for example that $\sqrt[3]{2}+\sqrt[5]{7}$ is algebraic of degree ≤ 15 over $\mathbb{Q}$. A more general statement is that the complex numbers which are algebraic over a subfield K of $\mathbb{C}$ form a field (called the algebraic closure of K in $\mathbb{C}$).

A polynomial having $a+b$, ab etc. as a root can be computed using resultants (see Exercise 4.8).

4.7 Construction of an Extension by Adjoining a Root

So far in this chapter, we have considered a very particular situation, namely, the case where K is a subfield of a field L, and we have defined what it means for an element of L to be algebraic over K. Fields that are subfields of $\mathbb{C}$ correspond to this situation; it is the situation which Dedekind considered in 1871, when he gave the first definition of a field. Almost all the exercises in Chapters 4–12 concern this situation. However, it is also possible to consider the following more general situation: K is an arbitrary field and P is a polynomial $K[X]$ that has no roots in K. Then, even without knowing any extension of K beforehand (see, for example, Chapter 14), we can construct an extension L of K in which P has at least one root. This more general situation was studied by Leopold Kronecker and Henri Weber in the years 1880 to 1900.

4.7.1 Definition

Let K be a field, and let P be a polynomial in $K[X]$. An extension L of K is called a *rupture field of P over K* if there exists a root x of P in L and if $L = K[x]$.

EXAMPLE. – $\mathbb{Q}[\sqrt[3]{2}]$ and $\mathbb{Q}[j\sqrt[3]{2}]$ are rupture fields of X^3-2 over $\mathbb{Q}$.

4.7.2 Proposition

Let P be an irreducible polynomial of degree n in $K[X]$. The quotient ring $L = K[X]/(P)$ is a rupture field of P, i.e. an extension of degree n of K containing the class x of X as a root of P. Moreover, P is the minimal polynomial of x over K.

PROOF. – It suffices to show that the ideal (P) is maximal; we will prove this so as to give a method making it possible to compute the inverse of a non-zero element of the quotient. Let $\pi : K[X] \to L$ denote the canonical projection. Every non-zero element of L is of the form $\pi(S)$ with S in $K[X]$ not a multiple of P. Consequently, because P is irreducible, P and S are relatively prime, and by Bézout's theorem, there exist U and V in $K[X]$ such that $US + VP = 1$. Thus we have $\pi(U)\pi(S) = 1$ in L, which shows that $\pi(S)$ is invertible, so L is a field.

Let $i : K \to L$ denote the composition of the injection $K \to K[X]$ and π. Since i is a homomorphism of rings with unit, it is injective, so L is an extension of K. Set $x = \pi(X)$ and $P = \sum_{0 \le k \le n} a_k X^k$. The polynomial P has coefficients in K, so we have $P(x) = \sum_{0 \le k \le n} a_k x^k = \pi(P) = 0$. Thus, x is algebraic over K. If a polynomial S in $K[X]$ vanishes at x, we have $S(x) = S(\pi(X)) = \pi(S) = 0$, so S is a multiple of P in $K[X]$. Consequently, P is the minimal polynomial of x over K. ♢

By §4.5.3, every element of L can be written uniquely as $\sum_{0 \le k < n} a_k x^k$. In other words, the set $\{1, x, \ldots, x^{n-1}\}$ forms a basis of L as a K-vector space.

4.7.3 Corollary

Let K be a field and P a non-constant polynomial of $K[X]$. Then there exists a rupture field L of P over K such that $[L : K] \le \deg(P)$.

PROOF. – Consider an irreducible factor p of P, and set $L = K[X]/(p)$, $\pi : K[X] \to L$, $x = \pi(X)$. We have $p(x) = 0$. The extension L of K contains a root of p, so it contains a root of P. ♢

4.7.4 Universal Property of $K[X]/(P)$

Let P be an irreducible polynomial of degree n of $K[X]$. The extension $K \to K[X]/(P)$ has a universal property which is an immediate consequence of the universal property of quotients.

PROPOSITION. – *For every extension M of K and every root a of P in M, there exists a unique field homomorphism $\varphi : K[X]/(P) \to M$ such that $\varphi(x) = a$ and $\varphi|K = id$ (in Chapter 6, we will say that φ is a K-homomorphism).*

PROOF. – Consider the ring homomorphism $f : K[X] \to M$ defined by $f|K : K \to M$ and $f(X) = a$. We have $f(P) = P(a) = 0$ so $f|(P) = 0$,

which gives the factorization of f by $K[X]/(P)$ by the universal property of quotients. $\diamondsuit$

EXAMPLES. – Set $P = X^2 - 2$, $K = \mathbb{Q}$, $M = \mathbb{R}$. Because P has two roots in $\mathbb{R}$, there exist two $\mathbb{Q}$-homomorphisms $\varphi, \varphi' : K = \mathbb{Q}[X]/(X^2 - 2) \to \mathbb{R}$; one sends x to $\sqrt{2}$, and the other to $-\sqrt{2}$.

For $P = X^3 - 2$, $K = \mathbb{Q}$, $M = \mathbb{R}$, there exists a unique $\mathbb{Q}$-homomorphism $\varphi : \mathbb{Q}[X]/(X^3 - 2) \to \mathbb{R}$, which sends x to $\sqrt[3]{2}$. However, if $M = \mathbb{C}$, there exist three $\mathbb{Q}$-homomorphisms $\varphi : \mathbb{Q}[X]/(X^3 - 2) \to \mathbb{C}$, defined by $\varphi(x) = \sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}$.

Toward Chapters 5 and 6

In order to prove the impossibility of certain geometric constructions that were sought for over 2000 years, it suffices to use just a part of the results of this chapter. These problems and the proofs of their impossibility form the subject of Chapter 5, which should be considered as a joyous digression. We will return to Galois theory proper in Chapter 6.

Exercises for Chapter 4

We found it natural, in a chapter concerning algebraic numbers, to present some of the famous and little taught examples of transcendental numbers. We follow the proofs given in Alan Baker's book listed in the bibliography.

Exercise 4.1. An example of a transcendental number: $\sum_{n>0} a_n 10^{-n!}$

1) Liouville's Theorem. Let a be a real number that is algebraic over $\mathbb{Q}$ of degree $n > 1$, and let P be an irreducible polynomial of degree n in $\mathbb{Z}[X]$ having a as a root. Show that there exists a real number $c > 0$ such that for every rational number p/q (with $q > 0$) we have $|a - (p/q)| > (c/q^n)$. We distinguish the two cases $|a - (p/q)| > 1$ and $|a - (p/q)| \leq 1$; in the second case, apply the mean value theorem and give an upper bound for $|P'|$ on the interval $[a - 1, a + 1]$.

2) Deduce the transcendence of $a = \sum_{n>0} a_n 10^{-n!}$ for every sequence (a_n) of natural numbers between 1 and 9.

Exercise 4.2. The transcendence of e

As in the previous exercise, we will assume that e is algebraic; we will obtain a double inequality (see **3)** and **4)** below) which can never be simultaneously satisfied.

Suppose that e is algebraic over $\mathbb{Q}$, a root of the irreducible polynomial $\sum_{0\le k\le n} q_k X^k$ in $\mathbb{Z}[X]$.

If $P(X) = \sum_{0\le k\le N} a_k X^k$ is a polynomial of $\mathbb{Z}[X]$, set

$$P_1(X) = \sum_{0\le k\le N} |a_k| X^k,$$

and for every real t, set

$$I(t) = \int_0^t \mathrm{e}^{t-u} P(u)\mathrm{d}u \quad \text{and} \quad J = \sum_{0\le k\le n} q_k I(k).$$

1) Show that $I(t) = \mathrm{e}^t \sum_{0\le k\le N} P^{(k)}(0) - \sum_{0\le k\le N} P^{(k)}(t)$.

Show that $|I(t)| \le |t|\mathrm{e}^{|t|} P_1(|t|)$.

2) From now on, let $P(X) = X^{p-1}(X-1)^p \dots (X-n)^p$, where p is a prime number $> n$. Show that

$$P^{(k)}(0) = \dots = P^{(k)}(n) = 0 \quad \text{for } k < p-1,$$
$$P^{(p-1)}(1) = \dots = P^{(p-1)}(n) = 0,$$
$$P^{(k)}(0), \dots, P^{(k)}(n) \quad \text{are divisible by } p! \text{ for } k \ge p.$$

3) A lower bound for J:

Show that $J = -q_0 \sum_{0\le k\le N} P^{(k)}(0) - \dots - q_n \sum_{0\le k\le N} P^{(k)}(n)$.

Deduce that $|J| \ge (p-1)!$ for $p > q_0$, by checking that $J = 0 \bmod (p-1)!$ and $J \ne 0 \bmod p!$.

4) An upper bound for J:

a) Show that $P_1(k) < (2n)^N$ for $0 \le k \le n$.

b) Deduce that $|J| \le A \cdot B^p$, where A and B are numbers not depending on p.

5) Conclude that e is transcendental.

Exercise 4.3. Determination of the rational roots of a polynomial with integral coefficients

1) Consider a polynomial $P(X) = \sum_{0 \le k \le n} a_k X^k \in \mathbb{Z}[X]$. Show that the rational roots of P are of the form $\frac{p}{q}$ such that p and q are relatively prime, p divides a_0 and q divides a_n.

2) Study the irreducibility of $X^3 - 4X^2 - \frac{9}{2}X - \frac{5}{2}$ in $\mathbb{Q}[X]$.

3) Study the irreducibility of $30X^3 + 277X^2 - 31X - 28$ in $\mathbb{Q}[X]$.

Exercise 4.4. Factorization of polynomials

1) For a prime p, show the irreducibility over $\mathbb{Q}$ of the cyclotomic polynomial
$$\Phi_p(X) = \sum_{0 \le k \le p-1} X^k$$
by applying Eisenstein's criterion to $\Phi_p(X+1)$.

2) Study the irreducibility of $X^6 + 3$ in the rings $\mathbb{Q}[X]$, $\mathbb{Q}[j][X]$, $\mathbb{Q}[i][X]$ (you will need at least a little background knowledge on factorial rings to solve the problem quickly over the third ring).

3) Study the irreducibility of $X^4 + 1$ in $\mathbb{Q}[X]$ (use the variable change $Y = X + 1$).

   Factorize $X^4 + 1$ into a product of irreducible factors in $\mathbb{Q}[\zeta][X]$, where ζ is a root of this polynomial.

4) Study the irreducibility of $P(X) = X^5 - X + 1$ in the ring $\mathbb{Q}[X]$ (show, for example, that P has no linear factor in $\mathbb{Z}[X]$, and then determine the quadratic polynomials S which could divide P in $\mathbb{Z}[X]$ by studying the values these candidates can take at -1, 0, 1).

5) Study the irreducibility of $P(X) = X^4 - 15X^3 + 7$ in the ring $\mathbb{Q}[X]$.

6) Let p be a prime number and $n \ge 2$ an integer. Show that $P(X) = X^n + pX + p^2$ is irreducible in $\mathbb{Z}[X]$.

7) Give an example of an irreducible quadratic polynomial P in $\mathbb{Q}[X]$ such that $P(X^2)$ is reducible in $\mathbb{Q}[X]$.

Exercise 4.5. The degree of an algebraic extension

Determine the degrees of the following extensions by finding bases for them, and answer the questions.

1) $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt[3]{2}]$ over $\mathbb{Q}$.

2) $\mathbb{Q}[\sqrt[3]{2}, \sqrt{2}]$ over $\mathbb{Q}[\sqrt[3]{2}]$, over $\mathbb{Q}[\sqrt{2}]$, over $\mathbb{Q}$.

3) $\mathbb{Q}[\sqrt{3}, \sqrt{2}]$ over $\mathbb{Q}[\sqrt{3}]$, over $\mathbb{Q}[\sqrt{2}]$, over $\mathbb{Q}$.

Compare $\mathbb{Q}[\sqrt{3}, \sqrt{2}]$ with $\mathbb{Q}[\sqrt{3} + \sqrt{2}]$. Determine the minimal polynomial of $\sqrt{3} + \sqrt{2}$ over $\mathbb{Q}$.

4) $\mathbb{Q}[j]$ over $\mathbb{Q}$.

Does $\sqrt{3}$ lie in $\mathbb{Q}[j]$? Does i lie in $\mathbb{Q}[j]$? Does j lie in $\mathbb{Q}[i]$?

$\mathbb{Q}[\sqrt{3}, j]$, $\mathbb{Q}[\sqrt{3}, i, j]$, $\mathbb{Q}[\sqrt{3}, i]$, $\mathbb{Q}[\sqrt{3} + i]$ over $\mathbb{Q}$.

5) $\mathbb{Q}[\cos \frac{2\pi}{3}]$, $\mathbb{Q}[\sin \frac{2\pi}{3}]$, $\mathbb{Q}[\cos \frac{2\pi}{5}]$, $\mathbb{Q}[\sin \frac{2\pi}{5} t]$ over $\mathbb{Q}$.

6) $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$ over $\mathbb{Q}$.

Exercise 4.6. Computing in algebraic extensions

Consider the polynomial $P(X) = X^3 + 2X + 2$ in $\mathbb{Q}[X]$; let a denote one of its roots.

1) Show that P is irreducible.

2) Express the elements $1/a$, $1/(a^2 + a + 1)$ and $u = a^6 + 3a^4 + 2a^3 + 6a$ as functions of 1, a, a^2 (for the quotients, use Euclid's algorithm and the method of indeterminate coefficients).

3) Determine the minimal polynomial of u over $\mathbb{Q}$.

Exercise 4.7. Algebraic extensions

1) Let L be an extension of finite degree n of a field K.

   a) What happens in the case $n = 1$? What happens if L' is another extension of K, contained in L and of degree n over K?

   b) Show that if n is prime, there exists no field strictly containing K and strictly contained in L.

2) Let K be a field, and let a be an algebraic element of degree n and of minimal polynomial P over K. Let b be an algebraic element over K whose degree m is relatively prime to n.

Determine the degree of $K[a, b]$ over K and show that P is irreducible over $K[b]$. What is the intersection $K[a] \cap K[b]$?

3) Let x be an algebraic element of odd degree over a field K. Show that x^2 is algebraic over K and that $K[x] = K[x^2]$.

4) Let K be a field, L an extension of K of finite degree n and a an element of L which is algebraic over K of minimal polynomial P over K. Show that $\deg(P)$ divides n.

5) Show that every quadratic extension of $\mathbb{Q}$ is of the form $\mathbb{Q}[\sqrt{a}]$, where a is a squarefree relative integer.

6) What are the algebraic extensions of $\mathbb{C}$? Give an example of an infinite degree extension of $\mathbb{C}$.

7) Let K be a field contained in $\mathbb{C}$, and let L be an algebraic (but not necessarily finite) extension of K. Let a be an element of $\mathbb{C}$ algebraic over L. Show that a is an algebraic element over K.

8) Show that e and π are transcendental over every algebraic extension of $\mathbb{Q}$.

Exercise 4.8. Elimination

1) Let K be a field contained in $\mathbb{C}$, and let a and b be two algebraic numbers over K, roots of two polynomials F and G respectively in $K[X]$. Set $\deg(G) = n$, and assume that there exists an algebraically closed field containing $K(Z)$.

a) Show that $R(Z) = \mathrm{Res}_X(F(X), G(Z - X))$ is a polynomial of $K[Z]$ having $a + b$ as a root.

b) More generally, show that if $T(X,Y) \in A[X,Y]$, then

$$R(Z) = \mathrm{Res}_X(F(X), \mathrm{Res}_Y(Z - T(X,Y), G(Y)))$$

is a polynomial in $K[Z]$ having $T(a,b)$ as a root.

c) Show that $R(Z) = \mathrm{Res}_X\left(F(X), X^n G(Z/X)\right)$ is a polynomial of $K[Z]$ having ab as a root.

d) If $T(Y) \in K[Y]$, give a non-zero polynomial which vanishes at $T(a)$.

2) Either directly or using results from the preceding problem, determine polynomials which are minimal polynomials over $\mathbb{Q}$ for the following numbers: $(2/3) + \sqrt{5/7}$, $\sqrt{2} + \sqrt[3]{3}$, $\sqrt{2} + \sqrt[4]{2}$, $a + \sqrt{2}$ where a is a root of $X^3 + X + 1$, and $b^2 + b$ where b is a root of $X^3 + 3X + 3$.

Solutions to Some of the Exercises

Solution to Exercise 4.3.

1) If p/q is a root of P, we have $q^n P(p/q) = 0$, i.e. $\sum_{0\le k\le n} a_k p^k q^{n-k} = 0$.

This produces the two inequalities

$$\begin{aligned} p \sum_{1\le k\le n} a_k p^{k-1} q^{n-k} &= -a_0 q^n, \\ q \sum_{0\le k\le n-1} a_k p^k q^{n-k-1} &= -a_n p^n, \end{aligned}$$

which give the result.

2) The only possible rational roots of $2X^3 - 8X^2 - 9X - 5$ are ± 5, ± 1, $\pm(1/2)$, $\pm(5/2)$. We see that 5 is a root, divide by it and complete the factorization.

3) This question needs more work than does the preceding one. First determine that $-(28/3)$ is a root, and then check that the factorization is given by $(3X + 28)(10X^2 - X - 1)$.

Solution to Exercise 4.4.

1) By Eisenstein's criterion, the polynomial

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{X+1-1} = \sum_{1\le k\le p} \binom{p}{k} X^{k-1}$$

is irreducible, since the formula $k!(p-k)!\binom{p}{k} = p!$ shows that the $\binom{p}{k}$ are divisible by p for $1 \le k \le p-1$ and that $\binom{p}{p} = 1$, $\binom{p}{1} = p$. It follows that Φ_p is irreducible. This classical result is generalizable to all cyclotomic polynomials (see Chapter 9).

2) Applying Eisenstein's criterion with the prime number $p = 3$, we see that the polynomial $X^6 + 3$ is irreducible in $\mathbb{Q}[X]$.

As $X^6 + 3 = (X^3 + i\sqrt{3})(X^3 - i\sqrt{3})$ and $i\sqrt{3} = 2j + 1$, the polynomial $X^6 + 3$ is not irreducible in $\mathbb{Q}[j][X]$; we have $X^6 + 3 = (X^3 + 2j + 1)(X^3 - 2j - 1)$.

The polynomial $X^6 + 3$ has coefficients in the factorial ring $\mathbb{Z}[i]$, whose fraction field is $\mathbb{Q}[i]$.

Let us show that the prime $p = 3$ is irreducible in $\mathbb{Z}[i]$. If we write $3 = (a + ib)(c + id)$ with $a, b, c, d \in \mathbb{Z}$, then taking moduli, we find that $9 = (a^2 + b^2)(c^2 + d^2)$. It is impossible to realize $a^2 + b^2 = 3$ or $c^2 + d^2 = 3$

in $\mathbb{Z}$, so $a+ib$ or $c+id$ has modulus 1, and it is invertible in $\mathbb{Z}[i]$. As 3 is irreducible in the factorial ring $\mathbb{Z}[i]$, it is prime in $\mathbb{Z}[i]$.

Applying Eisenstein's criterion, we then see that the polynomial X^6+3 is irreducible in $\mathbb{Q}[i][X]$.

Because we know the factorization of X^6+3 into linear factors in $\mathbb{C}$, we can also show that X^6+3 has no factors of degree 1, 2, or 3 in $\mathbb{Q}[i][X]$, by trying to regroup two or three factors (and taking care not to forget any cases).

3) Eisenstein's criterion applies to $(X+1)^4+1$.

Solving $x^4 = -1 = \mathrm{e}^{i\pi}$ leads to setting $\zeta = \mathrm{e}^{i\pi/4} = (1+i)/\sqrt{2}$. The roots of X^4+1 are $\mathrm{e}^{i\pi/4}, e^{3i\pi/4} = \zeta^3, \mathrm{e}^{5i\pi/4} = \zeta^5, \mathrm{e}^{7i\pi/4} = \zeta^7$, so in the ring $\mathbb{Q}[\zeta][X]$ we have

$$X^4+1 = (X-\zeta)(X-\zeta^3)(X-\zeta^5)(X-\zeta^7).$$

Every other choice of ζ leads to the same result.

4) The method we propose below is Kronecker's algorithm (1882); generally, it is too long to be useful in practice.

The only possible rational roots of the polynomial are ±1, which obviously do not work. If X^5-X+1 is reducible in $\mathbb{Q}[X]$, it has a quadratic factor $T(X)$ that we can choose in $\mathbb{Z}[X]$. As $T(0)$, $T(1)$, and $T(-1)$ respectively divide $P(0)$, $P(1)$, and $P(-1)$, they are equal to ±1. The possible polynomials T are $\pm(2X^2-1)$, $\pm(X^2+X-1)$, $\pm(X^2-X-1)$, and we check that none of them divides $P(X)$.

5) If P is reducible in $\mathbb{Q}[X]$, it factors into a product of two non-constant monic polynomials in $\mathbb{Z}$. Consider the situation mod 2. The image P_1 of P in $(\mathbb{Z}/2\mathbb{Z})[X]$ is equal to X^4+X^3+1. As P_1 has no root in $\mathbb{Z}/2\mathbb{Z}$ (the only possible roots, 0 and 1, do not work), P_1 has no linear factor. Suppose that $P_1(X) = (X^2+aX+b)(X^2+cX+d)$; the equality $bd=1$ leads to $b=d=1$, then to $a+c=1$ and $a+c=0$, which are contradictory.

6) We denote the image of a polynomial in $\mathbb{Z}[X]$ in $(\mathbb{Z}/p\mathbb{Z})[X]$ by adding a subscript 1.

If $P=ST$ in $\mathbb{Z}[X]$, where S and T are non-invertible monic polynomials in $\mathbb{Z}[X]$ of degrees s and t respectively, we have $S_1T_1 = X^n$ so $S_1(X) = X^s$, $T_1(X) = X^t$, $S(X) = X^s + \sum\limits_{0\le k<s} pa_kX^k$, and $T(X) = X^t + \sum\limits_{0\le k<t} pb_kX^k$.

The value $s=1$ (and similarly, $t=1$) leads to a contradiction because the equality of the constant terms would give $a_0b_0 = 1$, so $a_0 = \pm1$ and $-pa_0 = \pm p$ would be a root of P, which is impossible.

Finally, $s,t>1$ is impossible, since the coefficient of X in the product is divisible by p^2.

7) If $P(X) = X^2-7X+1$, we have $P(X^2) = (X^2+3X+1)(X^2-3X+1)$.

Solution to Exercise 4.5.

1) $X^2 - 2$ and $X^3 - 2$ are irreducible over $\mathbb{Q}$ by Eisenstein's criterion with $p = 2$.

As the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $X^2 - 2$, we have

$$\left[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}\right] = 2$$

and a basis of $\mathbb{Q}[\sqrt{2}]$ over $\mathbb{Q}$ is given by $\{1, \sqrt{2}\}$.

As the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $X^3 - 2$, we have $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$, and a basis of $\mathbb{Q}[\sqrt[3]{2}]$ over $\mathbb{Q}$ is given by $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$.

2) $\mathbb{Q}[\sqrt[3]{2}, \sqrt{2}]$ is an extension of $\mathbb{Q}[\sqrt[3]{2}]$, of $\mathbb{Q}[\sqrt{2}]$, and of $\mathbb{Q}$ (Figure 4.3).

The tower rule gives

$$\begin{aligned}\left[\mathbb{Q}[\sqrt[3]{2}, \sqrt{2}] : \mathbb{Q}\right] &= \left[\mathbb{Q}[\sqrt[3]{2}, \sqrt{2}] : \mathbb{Q}[\sqrt{2}]\right]\left[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}\right].\\ &= \left[\mathbb{Q}[\sqrt[3]{2}, \sqrt{2}] : \mathbb{Q}[\sqrt[3]{2}]\right]\left[\mathbb{Q}[\sqrt[3]{2}], \mathbb{Q}\right],\end{aligned}$$

which proves that $\left[\mathbb{Q}[\sqrt[3]{2}, \sqrt{2}] : \mathbb{Q}\right]$ is a multiple of 2 and 3, so it is a multiple of 6.

As $\sqrt[3]{2}$ is of degree ≤ 3 over every field containing $\mathbb{Q}$, we have

$$\left[\mathbb{Q}[\sqrt[3]{2}, \sqrt{2}] : \mathbb{Q}\right] = \left[\mathbb{Q}[\sqrt[3]{2}, \sqrt{2}] : \mathbb{Q}[\sqrt{2}]\right]\left[\mathbb{Q}[\sqrt{2}, \mathbb{Q}]\right] \leq 6.$$

Finally, $\left[\mathbb{Q}[\sqrt[3]{2}, \sqrt{2}] : \mathbb{Q}\right] = 6$. Consequently, $\left[\mathbb{Q}[\sqrt[3]{2}, \sqrt{2}] : \mathbb{Q}[\sqrt{2}]\right] = 3$ and $\left[\mathbb{Q}[\sqrt[3]{2}, \sqrt{2}] : \mathbb{Q}[\sqrt[3]{2}]\right] = 2$.

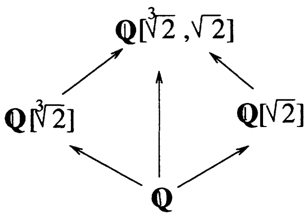


FIGURE 4.3.

A basis of $\mathbb{Q}[\sqrt[3]{2}, \sqrt{2}]$ over $\mathbb{Q}$ can be obtained from the bases $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ of $\mathbb{Q}[\sqrt[3]{2}]$ over $\mathbb{Q}$ and $\{1, \sqrt{2}\}$ of $\mathbb{Q}[\sqrt[3]{2}, \sqrt{2}]$ over $\mathbb{Q}[\sqrt[3]{2}]$. We obtain

$$\left\{1, \sqrt[3]{2}, \sqrt[3]{4}, \sqrt{2}, 2^{5/6}, 2^{7/6}\right\}.$$

As $2^{7/6} = 2 \times 2^{1/6}$, a simpler basis is given by $\left\{2^{k/6}, 0 \leq k \leq 5\right\}$. This last remark leads to the equality $\mathbb{Q}[\sqrt[3]{2}, \sqrt{2}] = \mathbb{Q}[\sqrt[6]{2}]$. We could have proved this equality directly by showing two easy converse inclusions.

3) In this case, we cannot use the same kind of reasoning as in the previous case, because the remark that $\left[\mathbb{Q}[\sqrt{3}, \sqrt{2}] : \mathbb{Q}\right]$ is a multiple of $\left[\mathbb{Q}[\sqrt{3}] : \mathbb{Q}\right]$ and of $\left[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}\right]$ only shows that $\left[\mathbb{Q}[\sqrt{3}, \sqrt{2}] : \mathbb{Q}\right]$ is a multiple of 2.

To see, for example, that $\left[\mathbb{Q}[\sqrt{3}, \sqrt{2}], \mathbb{Q}[\sqrt{2}]\right] = 2$, one must check that $\sqrt{3}$ is not in $\mathbb{Q}[\sqrt{2}]$. If $\sqrt{3} = a + b\sqrt{2}$, a and b in $\mathbb{Q}$, $3 = a^2 + 2b^2 + 2ab\sqrt{2}$. As $\left\{1, \sqrt{2}\right\}$ is a basis of $\mathbb{Q}[\sqrt{2}]$ over $\mathbb{Q}$, $ab = 0$; if $b = 0$, $3 = a^2$ is impossible. If $a = 0$, then $3 = 2b^2$ is impossible (see Exercise 2.1).

Finally, $[\mathbb{Q}[\sqrt{3}, \sqrt{2}] : \mathbb{Q}] = 4$. A basis of the extension is given by

$$\left\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\right\}.$$

The inclusion $\mathbb{Q}[\sqrt{3} + \sqrt{2}] \subset \mathbb{Q}[\sqrt{3}, \sqrt{2}]$ is obvious.

Conversely, $\sqrt{3}$ and $\sqrt{2}$ are in $\mathbb{Q}[\sqrt{3} + \sqrt{2}]$ because they are the half-sum and half-difference of $a = \sqrt{3} + \sqrt{2}$ and its inverse $\sqrt{3} - \sqrt{2}$.

The minimal polynomial of $\sqrt{3} + \sqrt{2}$ over $\mathbb{Q}$ (which by the above is a degree 4 polynomial) is obtained by setting $a = \sqrt{3} + \sqrt{2}$, giving $a^2 = 5 + 2\sqrt{6}$, $a^4 - 10a^2 + 1 = 0$. The desired polynomial is $X^4 - 10X^2 + 1$.

4) As j is not real, its degree over $\mathbb{Q}$ is ≥ 2. We know that $j^2 + j + 1 = 0$, so the minimal polynomial of j over $\mathbb{Q}$ is $X^2 + X + 1$. A basis of $\mathbb{Q}[j]$ over $\mathbb{Q}$ is $\{1, j\}$.

In what follows, note that two quadratic extensions $\mathbb{Q}[a]$ and $\mathbb{Q}[b]$ are equal whenever $a \in \mathbb{Q}[b]$.

If $\sqrt{3} \in \mathbb{Q}[j]$, we would have $\mathbb{Q}[j] = \mathbb{Q}[\sqrt{3}] \subset \mathbb{R}$, which is false. Similarly, $i \in \mathbb{Q}[j]$ and $j \in \mathbb{Q}[i]$ are impossible, since $2j + 1 = i\sqrt{3}$ would imply that $\mathbb{Q}[i] = \mathbb{Q}[j] = \mathbb{Q}[\sqrt{3}]$.

As j is not real, we are sure that it is of degree 2 over $\mathbb{Q}[\sqrt{3}]$ (of minimal polynomial $X^2 + X + 1$ over $\mathbb{Q}[\sqrt{3}]$). Hence $[\mathbb{Q}[\sqrt{3}, j] : \mathbb{Q}[\sqrt{3}]] = 2$, then $[\mathbb{Q}[\sqrt{3}, j] : \mathbb{Q}] = 4$, and finally $[\mathbb{Q}[\sqrt{3}, j] : \mathbb{Q}[j]] = 2$, which means that $\sqrt{3}$ is of degree 2 over $\mathbb{Q}[j]$.

A basis of $\mathbb{Q}[\sqrt{3}, j]$ over $\mathbb{Q}$ is $\{1, \sqrt{3}, j, j\sqrt{3}\}$.

It is clear that $\mathbb{Q}[\sqrt{3}, j] \subset \mathbb{Q}[\sqrt{3}, i, j]$; furthermore, $i = (2j+1)/\sqrt{3}$ shows that $i \in \mathbb{Q}[\sqrt{3}, j]$, so that $\mathbb{Q}[\sqrt{3}, j] = \mathbb{Q}[\sqrt{3}, i, j]$.

We check similarly that $\mathbb{Q}[\sqrt{3}, j] = \mathbb{Q}[\sqrt{3}, i] = \mathbb{Q}[i, j]$.

Finally, if $a = i + \sqrt{3}$, we have $(a - i)^2 = 3$, $(a - \sqrt{3})^2 = -1$, which gives i and $\sqrt{3}$ in terms of a, and $\mathbb{Q}[i + \sqrt{3}] = \mathbb{Q}[i, \sqrt{3}]$ of degree 4 over $\mathbb{Q}$.

Two other bases of $\mathbb{Q}[\sqrt{3}, j]$ over $\mathbb{Q}$ are thus given by

$$\left\{1, \sqrt{3}, i, i\sqrt{3}\right\}, \quad \left\{1, i, j, ij\right\}.$$

5) We have

$$\mathbb{Q}[\cos\frac{2\pi}{3}] = \mathbb{Q}[-\frac{1}{2}] = \mathbb{Q}$$

and

$$\mathbb{Q}[\sin\frac{2\pi}{3}] = \mathbb{Q}[\sqrt{3}].$$

Let $\zeta = e^{2i\pi/5}$. As ζ is a root of the polynomial $X^4 + X^3 + X^2 + X + 1$, which is irreducible over $\mathbb{Q}$, ζ is of degree 4 over $\mathbb{Q}$.

Set $a = 2\cos(2\pi/5) = \zeta + \zeta^4$. We have $a^2 = \zeta^2 + \zeta^3 + 2 = -a + 1$; a is a root of $X^2 + X - 1$, so $a = (-1 \pm \sqrt{5})/2$. As $\cos(2\pi/5) > 0$, we see that $\cos(2\pi/5) = (-1+\sqrt{5})/4$, so $\mathbb{Q}[\cos(2\pi/5)] = \mathbb{Q}[\sqrt{5}]$. As $2\cos(2\pi/5) = \zeta + \zeta^4$, we have $\mathbb{Q}[\cos(2\pi/5)] \subset \mathbb{Q}[\zeta]$ and $[\mathbb{Q}[\zeta] : \mathbb{Q}[\cos(2\pi/5)]] = 2$ (Figure 4.4).

It follows that $\sin(2\pi/5) = \sqrt{1-\cos^2(2\pi/5)} = \sqrt{(10+2\sqrt{5})/4}$, since $\sin(2\pi/5)$ is > 0. It is not obvious that $\sin(2\pi/5)$ is of degree 4 over $\mathbb{Q}$, but if we set $b = 2\sin(2\pi/5)$, we have $b^2 = 10 + 2\sqrt{5}$, so $b^4 - 5b^2 + 5 = 0$ and Eisenstein's criterion works with $p = 5$. As $\sqrt{5} \in \mathbb{Q}[\sin(2\pi/50]$, $\mathbb{Q}[\sin(2\pi/5)]$ is a quadratic extension of $\mathbb{Q}[\cos(2\pi/5)]$. Note that $\mathbb{Q}[\zeta, i] = \mathbb{Q}[\zeta, \sin(2\pi/5)]$.

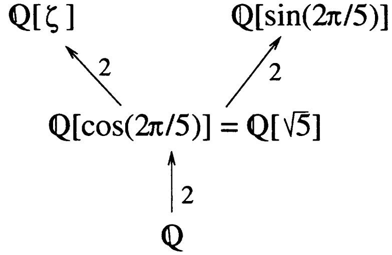


FIGURE 4.4.

6) To show that $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$ is of degree 8 over $\mathbb{Q}$, it suffices to show that $\sqrt{5}$ is of degree 2 over $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

If $\sqrt{5} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ for rational numbers a, b, c, d, squaring gives an equality in $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ which, using the fact that 1, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$ forms a basis, implies that

$$\begin{aligned} ba + 3cd &= 0, \\ ca + 2bd &= 0, \\ ad + bc &= 0, \\ a^2 + 2b^2 + 3c^2 + 6d^2 &= 5. \end{aligned}$$

The first two equations give a linear system in a and d. Its determinant is $2b^2 - 3c^2$, which is zero only if $b = c = 0$. In this case, a or d is zero by the third equation, and $5 = a^2 + 6d^2$ is impossible. If $2b^2 - 3c^2 \neq 0$, then $a = d = 0$, b or c is zero by the third equation, and $5 = 2b^2 + 3c^2$ is impossible.

Later (Exercise 8.10), we will see a generalization of this result to the degree of an extension of $\mathbb{Q}$ by a finite set of square roots of distinct prime numbers.

Solution to Exercise 4.6.

1) Use Eisenstein's criterion or check that P has no rational root: the only possible roots would be ± 1, ± 2, and they do not work.

2) The equality $a^3 + 2a + 2 = 0$ immediately gives the inverse of a since it implies that $a\left(-(a^2/2) - 1\right) = 1$, so that $(1/a) = -(a^2/2) - 1$.

The inverse of $a^2 + a + 1$ can be found by the method of indeterminate coefficients or the method of successive Euclidean division (see §4.5.2):

$$\begin{aligned} X^3 + 2X + 2 &= (X^2 + X + 1)(X - 1) + 2X + 3, \\ X^2 + X + 1 &= (2X + 3)(\frac{X}{2} - \frac{1}{4}) + \frac{7}{4}, \end{aligned}$$

gives Bézout's identity

$$\frac{7}{4} = -\left(\frac{X}{2} - \frac{1}{4}\right)(X^3 + 2X + 2) + (X^2 + X + 1)\frac{2X^2 - 3X + 5}{4}.$$

It follows that $1/(a^2 + a + 1) = (2a^2 - 3a + 5)/7$.

This last computation can be done by Euclidean division:

$$X^6 + 3X^4 + 2X^3 + 6X = (X^3 + 2X + 2)(X^3 + X) - 2X^2 + 4X,$$

so $u = -2a^2 + 4a = 2a(2 - a)$.

Alternatively, we can compute using a table of the a^n expressed in terms of basis vectors (Table 4.1 below), which is a good way of computing in an extension when one does not have a computer package for formal computation at one's disposal.

	1	a	a^2
1	1		
a		1	
a^2			1
a^3	-2	-2	
a^4		-2	-2
a^5	4	4	-2
a^6	4	8	4

TABLE 4.1.

3) As u is not in $\mathbb{Q}$, it is of degree 3 over $\mathbb{Q}$, and we obtain its minimal polynomial over $\mathbb{Q}$ by computing the powers of u in the basis 1, a, a^2, using Table 4.2, and then looking for a linear combination of 1, u, u^2, u^3 equal to zero:

$$\alpha + \beta u + \gamma u^2 = u^3.$$

	1	a	a^2
1	1		
u		4	-2
u^2	32	24	8
u^3	32	192	64

TABLE 4.2.

We find

$$\begin{aligned} \alpha + 32\gamma &= 32, \\ 4\beta + 24\gamma &= 192, \\ -2\beta + 8\gamma &= 64. \end{aligned}$$

This gives $\alpha = -224$, $\beta = 0$, $\gamma = 8$, and the minimal polynomial of u is $X^3 - 8X^2 + 224$.

Solution to Exercise 4.7.

1) The first exercise is trivial, but its results are useful.

a) If $n = 1$, then $L = K$. If $L' \subset L$ and $[L' : K] = n$, we have $[L' : L] = 1$ so $L' = L$.

b) If $n = [L : K]$ is prime and $K \subset L' \subset L$, then $[L' : K]$ divides n so it is equal to 1 or n, and either $L' = K$ or $L' = L$ by **a)**.

2) We have already seen some examples of this reasoning; both $[K[a] : K]$ and $[K[b] : K]$ divide $[K[a,b] : K]$ which is thus a multiple of mn, and moreover, $[K[a,b] : K[a]] \leq [K[b] : K]$ implies that $[K[a,b] : K] \leq mn$. Finally, $[K[a,b] : K] = mn$, so $[K[a,b] : K[b]] = m$, and P is irreducible over $K[b]$.

As $[K[a] \cap K[b] : K]$ divides both $[K[a] : K]$ and $[K[b] : K]$, it is equal to 1 and we have $K[a] \cap K[b] = K$.

3) As $x^2 \in K[x]$, x^2 is algebraic over K and $K[x^2] \subset K[x]$. As x is a root of the polynomial $X^2 - x^2$ with coefficients in $K[x^2]$, x is algebraic of degree at most 2 over $K[x^2]$. Moreover, $[K[x] : K[x^2]]$ divides $[K[x] : K]$, which is odd, so it is equal to 1. Hence $K[x] = K[x^2]$. The minimal polynomial of x over K gives an expression for x in terms of x^2 by regrouping the terms of even order and the terms of odd order.

4) It suffices to note that $\deg(P) = [K[a] : K]$, so $\deg(P)$ divides n.

5) A quadratic extension of $\mathbb{Q}$ is an extension by a number of the form $(x \pm \sqrt{y})/2$ with x, y rational; thus it is an extension of the form $\mathbb{Q}[\sqrt{y}]$. If $y = m/n$ with m and n rational, then $\mathbb{Q}[\sqrt{y}] = \mathbb{Q}[\sqrt{mn}/n] = \mathbb{Q}[\sqrt{mn}]$.

If $mn = d^2a$ for a squarefree integer a, then

$$\mathbb{Q}[\sqrt{mn}] = \mathbb{Q}[d\sqrt{a}] = \mathbb{Q}[\sqrt{a}].$$

6) By d'Alembert's theorem, $\mathbb{C}$ has no algebraic extensions of finite degree except for itself. The field $\mathbb{C}(X)$ of rational functions with complex coefficients is an example of an extension of $\mathbb{C}$ that is not algebraic, and has infinite degree.

7) Let $P(X) = \sum_{0 \leq k \leq n} a_k X^k$ be the minimal polynomial of a over L. In fact, a lies in the extension $K[a_0, \ldots, a_n][a]$, which is an extension of finite degree of K since it is an extension of finite degree of $K[a_0, \ldots, a_n]$ and $K[a_0, \ldots, a_n]$ is an extension of finite degree of K (Figure 4.5). This solves the problem.

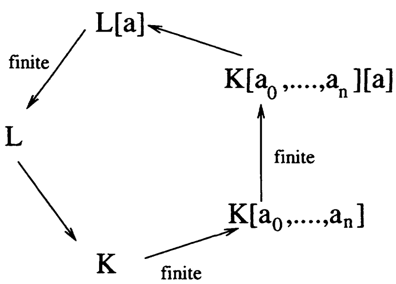


FIGURE 4.5.

8) Otherwise, e and π would be of finite degree over $\mathbb{Q}$, so they would be algebraic over $\mathbb{Q}$.

Solution to Exercise 4.8.

COMMENTARY. – To find a non-zero polynomial which vanishes at an algebraic number given as a polynomial function of other algebraic numbers, we can use resultants, but the polynomial we obtain may not be minimal.

1) a) To compute $\text{Res}_X(F(X), G(Z-X))$, we work with polynomials with coefficients in $K[Z]$, so that the resultant lies in the same ring. To show that $R(a+b) = 0$, it suffices to check that $F(X)$ and $G(a+b-X)$ have a common root, but a itself is such a root.

Note that even if F and G are the minimal polynomials of a and b, we do not necessarily find the minimal polynomial of $a+b$, as the degree of the resultant is the product of the degrees of a and b over K.

b) As $\mathrm{Res}_Y(Z - T(X,Y), G(Y))$ lies in $K[Z][X]$, $R(Z)$ lies in $K[Z]$.

For $Z = T(a,b)$, $F(X)$ and $\mathrm{Res}_Y(T(a,b) - T(X,Y), G(Y))$ are two polynomials in X having a a as a common root, since the two polynomials $T(a,b) - T(a,Y)$ and $G(Y)$ in Y have b as a common root.

c) ab is a root of $R(Z)$ since a is a common root of the polynomials $F(X)$ and $X^n G(ab/X)$.

d) We can take $R(Z) = \mathrm{Res}_X(F(X), Z - T(X))$ since $F(X)$ and $T(a) - T(X)$ have a as a common root.

2) These numbers lie in extensions of $\mathbb{Q}$ of degree $n = 2, 6, 4, 6, 3$, respectively. To find a polynomial that vanishes at these numbers, we can

a) look for a relation of linear dependence between the k-th powers of the numbers for $0 \leq k \leq n$, in a suitable extension of $\mathbb{Q}$;

b) use resultants as described above;

c) proceed more directly if the expression of the number allows this.

As $x = (2/3) + \sqrt{5/7}$ satisfies $(x - (2/3))^2 = (5/7)$, x is a root of $X^2 - (4/3)X - (17/63)$. As x is of degree 2 over $\mathbb{Q}$, because $\mathbb{Q}[x] = \mathbb{Q}[\sqrt{\frac{5}{7}}] = \mathbb{Q}[\sqrt{35}]$, this polynomial is the minimal polynomial of x over $\mathbb{Q}$.

If $y = \sqrt{2} + \sqrt[3]{3}$, $\left(y - \sqrt{2}\right)^3 = 3$, $y^3 + 6y - 3 = \sqrt{2}(3y^2 + 2)$ and squaring, we get $y^6 - 6y^4 - 6y^3 + 12y^2 - 36y + 1 = 0$. We can also obtain this result by computing $\mathrm{Res}_X(X^3 - 3, (Z - X)^2 - 2)$.

The polynomial $P(X) = X^6 - 6X^4 - 6X^3 + 12X^2 - 36X + 1$ is the minimal polynomial of y over $\mathbb{Q}$, which is of degree 6. There are several ways to prove that it is of degree 6. For example, note that y generates $\mathbb{Q}[\sqrt{2}, \sqrt[3]{3}]$ since $\sqrt{2} = (y^3 + 6y - 3)/(3y^2 + 2)$.

If $z = \sqrt{2} + \sqrt[4]{2}$, we have $\left(z - \sqrt{2}\right)^2 = \sqrt{2}$, so that $z^4 - 4z^2 - 8z + 2 = 0$. The corresponding polynomial is the minimal polynomial of z over $\mathbb{Q}$, which is irreducible by Eisenstein's criterion.

If $t = a + \sqrt{2}$, then $(t - \sqrt{2})^3 + t - \sqrt{2} + 1 = 0$, so that if we separate the terms containing $\sqrt{2}$ and square, we obtain $t^6 - 4t^4 + 2t^3 + 13t^2 + 14t - 17 = 0$. This is the minimal polynomial of t over $\mathbb{Q}$, by a reasoning analogous to the one used for y.

If $u = b^2 + b$, $u^2 = -6 - 9b - 2b^2$, $u^3 = 33 + 33b - 9b^2$ and $u^3 = \alpha + \beta u + \gamma u^2$ leads to a linear system whose solution gives $u^3 + 6u^2 + 21u + 3 = 0$. This is a minimal polynomial for u since b lies in a cubic extension of $\mathbb{Q}$ and not in $\mathbb{Q}$ (one can also use Eisenstein's criterion).

5

Constructions with Straightedge and Compass

For the ancient Greeks, a geometric construction was a construction done using only straightedge and compass (a "straightedge" is a ruler not marked with any measurements). In this chapter, we consider planar problems, in the sense of elementary geometry. The verb "construct" means construct with straightedge and compass, according to the procedures described more precisely below.

5.1 Constructible Points

Let E be a set of points in the plane. Write $\mathcal{D}_E$ for the set of lines in the plane passing through two distinct points of E, and let $\mathcal{C}_E$ denote the set of circles in the plane whose center is a point of E and whose radius is a distance between two distinct points of E.

DEFINITIONS. – A point of the plane is said to be *constructible in one step* from E if it is either

1) an intersection of two lines in $\mathcal{D}_E$,

2) an intersection of a line in $\mathcal{D}_E$ and a circle in $\mathcal{C}_E$, or

3) an intersection of two circles in $\mathcal{C}_E$.

A point P in the plane is said to be *constructible in n steps* from E if there exists a finite sequence $P_1, \ldots, P_n$ of points in the plane such that $P_n = P$ and for $i = 1, \ldots, n$, P_i is constructible in one step from $E \cup \{P_j; j < i\}$.

A point P in the plane is said to be *constructible from* E if there exists an integer n such that P is constructible in n steps from E.

REMARK. – If E contains only one element, then no new points can be constructed from it.

The number of steps depends on the construction procedure, though there exists a minimal such number.

5.2 Examples of Classical Constructions

5.2.1 Projection of a Point onto a Line

Let (AB) be a line passing through two points A and B, and let M be a point not on (AB). We construct the projection H of M onto (AB) from $\{A, B, M\}$ by the following steps:

1) draw the circle of center A and radius AM,

2) draw the circle of center B and radius BM that intersects the previous circle at N, and

3) draw the line (MN), that intersects the line (AB) at H (Figure 5.1).

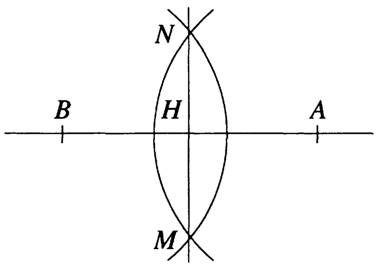


FIGURE 5.1. Construction of a projection

5.2.2 Construction of an Orthonormal Basis from Two Points

Let O and A be two distinct points in the plane which we assume to be at a distance of 1 from each other. We construct an orthonormal basis (O, A, B) from $\{O, A\}$ by the following steps:

1) draw the circle C of center O and radius OA, which intersects (OA) at A';

2) draw the circle of center A and radius AA';

3) draw the circle of center A' and radius AA', which intersects the previous circle at M and N; and

4) draw the line MN which intersects the circle C at B and B' (Figure 5.2).

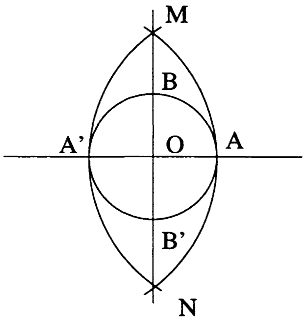


FIGURE 5.2. Construction of an orthonormal basis

REMARK. – Using the two above constructions together, we can construct the line perpendicular to a given line, passing through a given point which may or may not lie on the line.

5.2.3 Construction of a Line Parallel to a Given Line Passing Through a Point

Let (AB) be a line and M a point not on it. We construct the line parallel to (AB) passing through M from the set of points $\{A, B, M\}$ by the following steps:

1) draw the circle of center A and radius $R = AM$, which intersects (AB) at C and C';

2) draw the circle of center C and radius R; and

3) draw the circle of center M and radius R, which intersects the previous circle at A and N (Figure 5.3).

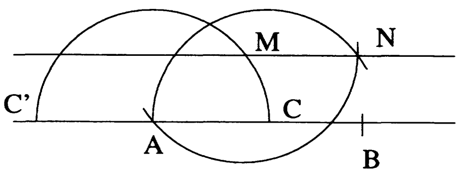


FIGURE 5.3. Construction of a line parallel to a given line

The desired line is then (MN).

5.3 Lemma

Let E be a set of points of the plane containing at least two elements O and A. Let B denote a point such that $\mathcal{R} = (O, A, B)$ is an orthonormal basis (which by §5.2.2 is constructible from O and A), and let $K = \mathbb{Q}(F)$ be the extension of $\mathbb{Q}$ generated by the set F of the (real) abscissas and ordinates of the points of E in this basis. Then

1) every line in $\mathcal{D}_E$ has an equation in $\mathcal{R}$ of the form

$$ax + by + c = 0 \qquad \textit{with} \quad a, b, c \in K;$$

2) every circle in $\mathcal{C}_E$ has an equation in $\mathcal{R}$ of the form

$$x^2 + y^2 + ax + by + c = 0 \qquad \textit{with} \quad a, b, c \in K.$$

PROOF. – If a line in $\mathcal{D}_E$ passes through two distinct points of E, with coordinates respectively given by (x_1, y_1) and (x_2, y_2) in the basis $\mathcal{R}$, then its equation is given by

$$(x - x_1)(y_2 - y_1) - (y - y_1)(x_2 - x_1) = 0,$$

which has the desired form.

Moreover, if a circle of $\mathcal{C}_E$ has center (x_0, y_0) in $\mathcal{R}$ and radius equal to the distance between two points of E with coordinates (x_1, y_1) and (x_2, y_2) in $\mathcal{R}$, then its equation is given by

$$(x - x_0)^2 + (y - y_0)^2 = (x_1 - x_2)^2 + (y_1 - y_2)^2,$$

which has the desired form. ♢

5.4 Coordinates of Points Constructible in One Step

PROPOSITION. – *Keep the notation of Lemma 5.3. If P is a point in the plane with coordinates (p, q) in $\mathcal{R}$, constructible in one step from E, then $K(p, q)$ is equal to K or to a quadratic extension of K.*

PROOF. – If P is the intersection of two lines in $\mathcal{D}_E$ given by equations

$$\begin{aligned} ax + by + c &= 0, \\ a'x + b'y + c' &= 0, \end{aligned}$$

with a, a', b, b', c, c' in K, then $ab' - a'b \neq 0$ since the two lines are not parallel; Cramer's rule then shows that p and q lie in K, so that $K(p, q) = K$.

If P is the intersection of a line in $\mathcal{D}_E$ and a circle in $\mathcal{C}_E$ given by equations

$$\begin{aligned} ax + by + c &= 0, \\ x^2 + y^2 + a'x + b'y + c' &= 0, \end{aligned}$$

with a, a', b, b', c, c' in K, we see that if $a \neq 0$, $p = -(bq + c)/a$ so p and q lie in the same extension of K. Then

$$(\frac{bq + c}{a})^2 + q^2 - a'\frac{bq + c}{a} + b'q + c' = 0$$

shows that q is a root of a quadratic polynomial $P \in K[X]$. The element q lies in K or in a quadratic extension of K according to whether P is not or is irreducible over K. If $a = 0$, then $b \neq 0$ and a similar reasoning holds.

If P is the intersection of two circles in $\mathcal{C}_E$ given by equations

$$\begin{aligned} x^2 + y^2 + ax + by + c &= 0, \\ x^2 + y^2 + a'x + b'y + c' &= 0, \end{aligned}$$

with a, a', b, b', c, c' in K, we reduce to the preceding case by noting that P is the intersection of the first circle with the line given by the equation

$$(a - a')x + (b - b')y + c - c' = 0. \qquad \diamond$$

5.5 A Necessary Condition for Constructibility

PROPOSITION. – *Keep the notation of Lemma 5.3. For every point $P = (p, q)$ constructible from E,*

1) *there exists a finite sequence of fields $(K_i)_{0 \leq i \leq m}$, each of which is a quadratic extension of the preceding one, with $K_0 = K$, $K_m \subset \mathbb{R}$, and $p, q \in K_m$; and*

2) *p and q are algebraic over K; their degrees over K are powers of 2.*

PROOF. –

1) We use induction on the number n of steps needed to construct P.

   If $n = 0$, the result is obvious.

   Suppose that for every point Q constructible in n steps from E, via the sequence of points $(Q_j)_{1 \leq j \leq n}$, there exists a finite increasing sequence $(K_s)_{0 \leq s \leq r}$ such that $K_0 = K$, $K_r \subset \mathbb{R}$, each field is quadratic over the preceding one and the coordinates of the Q_j, $1 \leq j \leq n$, lie in K_r.

If P is constructible in $n+1$ steps from E, there exists a sequence of points $(P_i)_{1 \leq i \leq n+1}$ such that $P_{n+1} = P$, and for $i = 0, \ldots, n$, P_{i+1} is constructible in one step from $E \cup \{P_j; j \leq i\}$. By the induction hypothesis, there exists a finite increasing sequence $(K_s)_{0 \leq s \leq r}$ such that $K_0 = K$, $K_r \subset \mathbb{R}$, each one is quadratic over the preceding one and the coordinates of the P_i, $1 \leq i \leq n$, lie in K_r. As the point P is constructible in one step from $E \cup \{P_i; i \leq n\}$, Proposition 5.4 applies (we add a term to the sequence if and only if p and q do not lie in K_r).

2) As $[K_i : K_{i-1}] = 2$ for $i \leq m$, the tower rule gives $[K_m : K] = 2^m$. This formula also shows that the degrees of p and q over K must divide 2^m, so they are powers of 2. ◇

5.6 Two Problems More Than Two Thousand Years Old

The second part of Proposition 5.5 provides a negative answer to problems set by the Greeks over two thousand years ago. This was first proved by Wantzel, who published his result in 1837 (although Gauss may have known it as early as 1796).

Par M. L. WANTZEL,

Élève-Ingénieur des Ponts-et-Chaussées.

Supposons qu'un problème de Géométrie puisse être résolu par des intersections de lignes droites et de circonférences de cercle : si l'on joint les points ainsi obtenus avec les centres des cercles et avec les points qui déterminent les droites on formera un enchaînement de triangles rectilignes dont les éléments pourront être calculés par les formules de la Trigonométrie ; d'ailleurs ces formules sont des équations algébriques qui ne renferment les côtés et les lignes trigonométriques des angles qu'au premier et au second degré ; ainsi l'inconnue principale du problème s'obtiendra par la résolution d'une série d'équations du second degré dont les coefficients seront fonctions rationnelles des données de la question et des racines des équations précédentes. D'après cela, pour reconnaître si la construction d'un problème de Géométrie peut s'effectuer avec la règle et le compas, il faut chercher s'il est possible de faire dépendre les racines de l'équation à laquelle il conduit de celles d'un système d'équations du second degré composées comme on vient de l'indiquer. Nous traiterons seulement ici le cas où l'équation du problème est algébrique.

FIGURE 5.4. The beginning of Wantzel's proof

5.6.1 Duplication of the Cube

A legend recounted by Eratosthene (around 276–196 B.C.) recounts that while the plague was raging in Delos, a small island of the Cyclades, Apollo's oracle declared that Apollo desired a cubic altar whose size was exactly the double of his former altar, and that he would stop the epidemic only when he determined that such a cubic altar had been built. Thus, the length of a side of the new altar was to be the length of a side of the old one multiplied by $\sqrt[3]{2}$.

It turns out to be impossible to construct a segment whose length is $\sqrt[3]{2}$ times a given length using only straightedge and compass. Indeed, this would be equivalent to constructing a point with coordinates $(\sqrt[3]{2}, 0)$ in an orthogonal basis constructed from O and A. But $\sqrt[3]{2}$ is of degree 3 over $\mathbb{Q}$. Of course, 3 does not divide any power of 2, so Proposition 5.5 shows that such a construction is impossible.

5.6.2 Trisection of the Angle

The trisection of the angle is the problem of dividing an arbitrary angle into three equal parts using only straightedge and compass. The ancient Greeks actually possessed other methods for trisecting angles (see Exercise 5.5).

Constructing an angle θ when its triple is known is equivalent to constructing the point $(\cos\theta, \sin\theta)$ of the unit circle in the plane, with respect to a basis $\mathcal{R} = (O, A, B)$, when the point $(\cos 3\theta, \sin 3\theta)$ is known. The formula $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ (due to Viète) shows that $\cos\theta$ is a root of the polynomial $4X^3 - 3X - \cos 3\theta$.

In general, this polynomial is irreducible over $\mathbb{Q}[\cos 3\theta]$; for example, when $\theta = 40°$, it is equivalent to $8X^3 - 6X + 1$, which is irreducible over $\mathbb{Q}$ because it has no rational roots. The same reasoning as in the preceding section then shows that the construction is impossible. It follows that angles of $(120/n)°$ for integers $n \geq 1$ are never "trisectable" (otherwise, the 120° angle would be).

5.7 A Sufficient Condition for Constructibility

PROPOSITION. – *Let us keep the notation of Lemma 5.3.*

1) *Every point with coordinates in $K = \mathbb{Q}(F)$ is constructible from E.*

2) *Every point whose coordinates lie in a quadratic extension of K is constructible from E.*

3) *Consider a point P with coordinates (p, q) such that there exists a finite increasing sequence of fields $(K_i)_{0 \leq i \leq m}$, each one quadratic over*

the preceding one, with $K_0 = K$, $K_m \subset \mathbb{R}$ *and* $p, q \in K_m$. *Then* P *is constructible from* E.

PROOF. –

1) Let p and q lie in K. To show that the point $P = (p, q)$ is constructible from E, it suffices, by §5.2.2, to show that the points $(p, 0)$ and $(0, q)$ are constructible from E. Let us show that $(p, 0)$ is constructible. By §4.3.1, p is of the form $S(a_1, \ldots, a_k)/T(a_1, \ldots, a_k)$, where k is an integer, S and T are polynomials in $\mathbb{Q}[X_1, \ldots, X_k]$, and $a_1, \ldots, a_k$ are elements of F. We construct $(p, 0)$ one step at a time by noting that if $(x, 0)$ and $(y, 0)$ are constructible from E, then $(-x, 0)$ and $(x + y, 0)$ are constructible from E (this is trivial), and also $(1/x, 0)$ and $(xy, 0)$ are constructible from E. Indeed, to construct $(1/x, 0)$, we construct the line that passes through the point $B = (0, 1)$ and is parallel to the line passing through $A = (1, 0)$ and $(0, x)$, and to construct $(xy, 0)$, we construct the line passing through $(0, y)$ and parallel to the line passing through the points B and $(x, 0)$ (Figure 5.5).

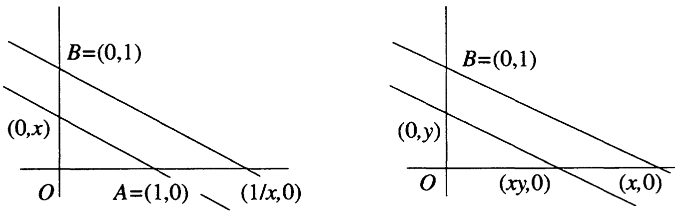


FIGURE 5.5. Construction of $(1/x,\ 0)$ and $(xy,\ 0)$

2) Let p be of degree 2 over K. Then p is a root of a quadratic polynomial T with coefficients in K. If $T(X) = X^2 + aX + b$, then

$$p = \frac{-a \pm \sqrt{a^2 - 4b}}{2};$$

if we set $c = a^2 - 4b$, the construction of $(p, 0)$ uses the construction of $(1, \sqrt{c})$ knowing $(c, 0)$.

We first construct the point $C = (c + 1, 0)$, the midpoint M of OC; to do this, construct the mediatrix of OC. Then we construct the intersection D of the circle of center M and radius MO with the line perpendicular to OA passing through A. Then $D = (1, \sqrt{c})$, so we conclude with the last step (Figure 5.6).

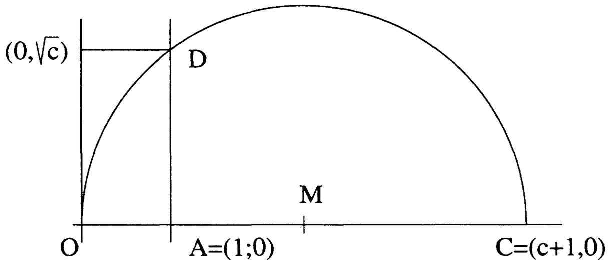


FIGURE 5.6. Constructions of $(0, \sqrt{c})$

3) This result is easily proved by induction, using the two previous results. This concludes the proof. ◇

COMMENTARY. – The constructions described above are given in the first pages of Descartes' *Geometry*. They enabled him to consider the product of two lengths x and y as a length, rather than considering it as the rectangle with sides x and y, and this led him to suppress the homogeneity conditions that had made the work of his predecessors so heavy: "...Où il est à remarquer que, par a^2, ou b^3, ou semblables, je ne conçois ordinairement que des lignes toutes simples, encore que pour me servir des noms usités en l'algèbre, je les nomme des carrés ou des cubes, etc." ("...it should be noted that, by a^2, or b^3, or others, I do not ordinarily conceive anything but perfectly simple lines, although in order to employ the names usual in algebra, I call them squares, cubes, etc.")

Exercises for Chapter 5

Exercise 5.1. Roots of quadratic equations

Let OAB denote an orthogonal basis of the plane.

1) Given two strictly positive real numbers s and p, construct the roots of the equation $X^2 - sX + p = 0$, starting by constructing a segment of length $\sqrt{p}$. Recover the usual algebraic condition geometrically.

2) Construct a segment of length $\sqrt[4]{2}$.

Exercise 5.2. Construction of the regular pentagon

1) Check the classical construction of the regular polygon with five sides, with one vertex labeled A, inscribed in a circle $\mathcal{C}$ of center O and radius OA.

   - Draw a diameter BB' perpendicular to OA.

- Let I denote the midpoint of OB'; draw the circle of center I and radius IA which intersects OB at D.
- The length of AD is equal to the length of the side of the regular pentagon to be constructed.

2) Construct a regular polygon with 30 sides using straightedge and compass.

COMMENTARY. – A different construction of the regular pentagon is given in book 4, proposition 11, of Euclid's *Elements* (around 300 B.C.). It is the climax of this part of the *Elements*; the propositions of books 2, 3, and 4 build methodically toward this end. The solution is entirely geometric.

Exercise 5.3. Constructible elements of degree 4

1) Let x be a complex number of degree 4 over $\mathbb{Q}$, and let $P(X) = X^4 + pX^2 + qX + r$ be its minimal polynomial over $\mathbb{Q}$. Show that there exists a quadratic extension L of $\mathbb{Q}$, contained in $\mathbb{Q}[x]$, if and only if the polynomial $R(X) = X^3 + 2pX^2 + (p^2 - 4r)X - q^2$ has a rational root.

2) Show that a real root of the polynomial $P(X) = X^4 + 2X - 2$ is not constructible.

Exercise 5.4. al Biruni's third-degree equation for the 20° angle

Let A and B denote two adjacent vertices of a regular 18-sided polygon inscribed in a circle of center O, as in Figure 5.7. The 10th century mathematician al Biruni constructed the isosceles triangles ABC with C on OB and $AB = AC$, ACD with D on OA and $AC = DC$, CDE with E on OA and $CD = DE$.

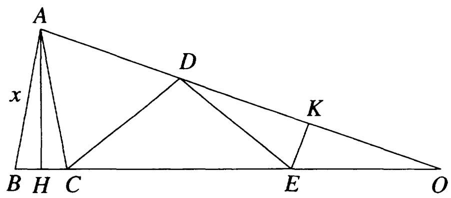


FIGURE 5.7. al Biruni's figure

1) Show that $OE = AB$.

2) Set $OA = 1$ and $AB = x$. Show that $x^3 + 1 = 3x$.

Exercise 5.5. Trisection of angles

1) Archimedes' method (Figure 5.8):

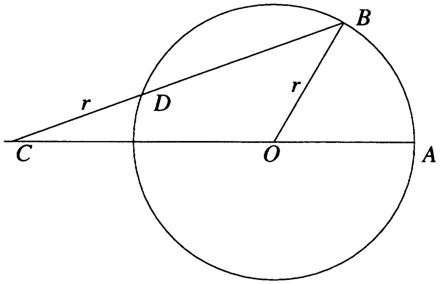


FIGURE 5.8. Archimedes' method

Consider a circle of center O and radius r, and an angle AOB where A and B are two points on the circumference of the circle. Suppose we are in possession of a straightedge marked with two points at a distance r from each other, and that with this straightedge, we know how to construct a line passing through B, intersecting the extension of the segment $[OA]$ toward O at C, and intersecting the circle at D in such a way that $[CD]$ is of length r.

Show that the angle DCO is one-third of the angle AOB.

2) Pappus' method.

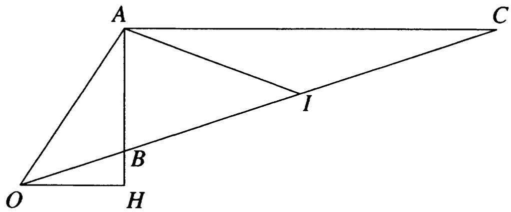


FIGURE 5.9. Pappus' method

Suppose we are given a right triangle AOH at H whose side $[OA]$ is of length a. Draw the line D parallel to (OH) passing through A. Suppose that we are in possession of a straightedge marked with two points at a distance of $2a$ from each other, and that with this straightedge, we know how to construct a line passing through O, intersecting the segment $[AH]$ at B and the line D at C in such a way that the length of the segment $[BC]$ is $2a$ (Figure 5.9).

Show that the angle BOH is equal to one-third of the angle AOH.

3) Origami (the Japanese art of paper-folding, called *kami* in Japanese).

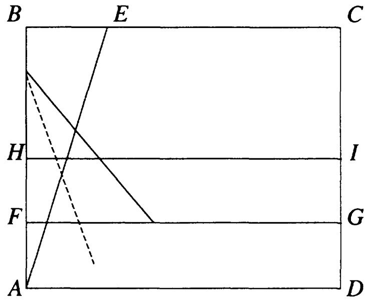


FIGURE 5.10. Trisection by origami

All straightedge and compass constructions can by done by origami, and many others as well. The origami method for trisecting an angle is due to the Japanese Abe. Take a rectangular piece of paper $ABCD$ and form the angle $\theta = DAE$ by folding along AE (Figure 5.10). By two successive foldings of an equal, arbitrary width, we obtain segments FG and HI parallel to AD such that $AF = FH$. Then fold in such a way as two simultaneously bring A to a point on FG and H to a a point of AE.

Show that the angle between AB and the axis of this last fold is equal to $\theta/3$.

Solutions to Some of the Exercises

Solution to Exercise 5.1.

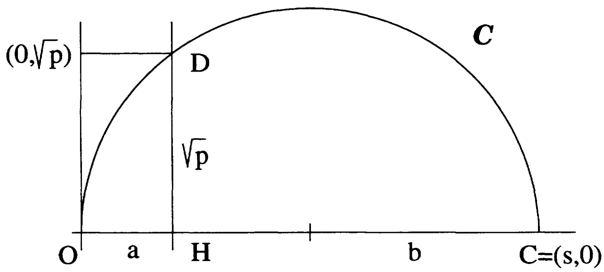


FIGURE 5.11. Construction of the roots of a quadratic equation

1) We first construct a segment of length $\sqrt{p}$ (see Proposition 5.7. 2)), and then a point C with coordinates $(s, 0)$ and a circle $\mathcal{C}$ of diameter OC. We construct a point D with ordinate $\sqrt{p}$ of $\mathcal{C}$, which projects to H on OC. The point H divides OC into segments of lengths a and b, which are the roots of the given equation.

The construction is possible on the one hand if $p \geq 0$, on the other hand if there exist points with ordinate $\sqrt{p}$ on the circle $\mathcal{C}$, i.e. $\sqrt{p} \leq s/2$; we recover the condition $s^2 - 4p \geq 0$.

2) We use the construction of Proposition 5.7 2) twice, first to construct a segment of length $\sqrt{2}$, and then to construct a segment whose length is a square root of $\sqrt{2}$.

Solution to Exercise 5.2.

1) Using Pythagorus' theorem, we easily compute AD; if $OA = 1$, it is $\sqrt{10 - 2\sqrt{5}}/2$ and we check that this is equal to $2\sin(\pi/5)$ by the identity

$$\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4} = 1 - 2\sin^2\frac{\pi}{5}$$

(see part 5) of Exercise 4.5).

2) Let D' denote an intersection of the circle of center A and radius AD with $\mathcal{C}$. The equality $\pi/15 = (2\pi/5) - (\pi/3)$ shows that an arc of the circle of center A and radius OA cuts the circle $\mathcal{C}$ at a point E between A and D' such that D' and E are adjacent vertices of a regular 30-sided polygon.

Solution to Exercise 5.3.

1) In the special case of a biquadratic equation, $q = 0$, $R(0) = 0$, and the intermediate extension always exists.

Assume the existence of L. The number x is of degree 2 over L; write $X^2 + aX + b$, with a, b in L for its minimal polynomial over L. This polynomial divides P in $L[X]$, so we have $P(X) = (X^2 + aX + b)(X^2 + cX + d)$, with c and d in L. By Descartes' method, we know that a^2 is a root of R. If a^2 is not rational, $\mathbb{Q}[a^2] = L$ so a^2 is of degree 2 over $\mathbb{Q}$, its minimal polynomial over $\mathbb{Q}$ divides R in $\mathbb{Q}[X]$, and thus R has a linear factor in $\mathbb{Q}[X]$, i.e. a rational root.

Conversely, if R has a rational root, there exists a decomposition of P in $\mathbb{Q}[X]$ into a product of the form $(X^2+aX+b)(X^2+cX+d)$, where a^2 is a rational root of R. Set $L = \mathbb{Q}[a]$. We know that L contains b, c, d, therefore x, a root of one of the two factors, is of degree ≤ 2 over L. As $[L : \mathbb{Q}] \leq 2$, we have $[L[x] : \mathbb{Q}] \leq 4$, and as $\mathbb{Q}[x] \subset L[x]$, we have $\mathbb{Q}[x] = L[x]$. We conclude that L gives the desired result.

2) P is irreducible by Eisenstein's criterion, and it has a real root since $P(0) = -2$, $P(1) = 1$. The corresponding polynomial R, equal to $X^3 + 8X - 4$, has no rational root, since the possible candidates ± 1, ± 2, ± 4 fail. We conclude by using 1) and the constructibility theorem.

6
K-Homomorphisms

In this chapter and the coming ones, we continue to restrict our attention to the situation of fields that can be realized as subfields of the field of complex numbers $\mathbb{C}$. However, the definitions and results all generalize directly to arbitrary fields contained in an algebraically closed field C of characteristic 0 (for fields of characteristic $p \neq 0$, see Chapters 14 and 15).

One surprising aspect of the theory is the very minor role played by polynomials, which appeared in previous chapters as the main subject of Galois theory. This is due to the efforts of Dedekind at the end of the 19th century, and Emil Artin in the 1920s and 1930s, to clarify the linear aspects of Galois theory – in particular, the notion of K-homomorphisms, which extends the original idea of permutations of roots of a polynomial.

6.1 Conjugate Numbers

DEFINITION. – Let K be a field, which as before we take to be an intermediate extension between $\mathbb{Q}$ and $\mathbb{C}$. Let a be a complex number that is algebraic over K, with minimal polynomial P over K. Each root of P in $\mathbb{C}$ is called a *conjugate* of a over K. Two roots of an irreducible polynomial of $K[X]$ are said to be conjugate over K.

EXAMPLES. –

1) The numbers i and $-i$ are conjugate over $\mathbb{Q}$ and over $\mathbb{R}$, but not over $\mathbb{C}$.

2) The numbers $\sqrt{2}$ and $-\sqrt{2}$ are conjugate over $\mathbb{Q}$, but not over $\mathbb{Q}[\sqrt{2}]$.

3) The numbers $\sqrt[3]{2}$, $j\sqrt[3]{2}$ and $j^2\sqrt[3]{2}$ are conjugate over $\mathbb{Q}$.

6.2 K-Homomorphisms

6.2.1 *Definitions*

Let K be a field, and let L and L' be two extensions of K contained in $\mathbb{C}$. A *K-homomorphism* from L to L' is a homomorphism of rings with unit from L to L', which leaves the elements of K invariant (i.e. whose restriction to K is the identity on K). In other words, a K-homomorphism is a homomorphism from the K-algebra L to the K-algebra L'.

We will often use the letter σ to denote a K-homomorphism. We will use the term K-isomorphism, respectively K-automorphism when σ is an isomorphism, respectively an automorphism.

EXAMPLES. –

1) Complex conjugation, which sends a complex number $a + ib$, with a and b real, to $a - ib$, is an $\mathbb{R}$-automorphism of $\mathbb{C}$; we will often consider its restriction to subfields.

2) The map $\sigma : \mathbb{Q}\left[\sqrt{2}\right] \to \mathbb{C}$ defined by $\sigma\left(a + b\sqrt{2}\right) = a - b\sqrt{2}$ with a and b rational, is a $\mathbb{Q}$-automorphism.

3) If L and L' are two extensions of K, and if K is an extension of K', then every K-homomorphism $\sigma : L \to L'$ is a K'-homomorphism, and in particular a $\mathbb{Q}$-homomorphism.

6.2.2 *Properties*

Let $\sigma : L \to L'$ be a K-homomorphism. It has the following properties:

1) it is a K-linear map between L and L' considered as K-vector spaces;

2) it is an injective map, like every ring homomorphism between two fields;

3) its image is a field $\sigma(L)$ which is K-isomorphic to L;

4) if L is of finite degree over K, a K-homomorphism $\sigma : L \to L$ is a K-automorphism of L, because since σ is a linear injective endomorphism of a finite-dimensional K-vector space, it must be surjective;

5) if $L = K[a_1, \dots, a_n]$, a K-homomorphism is defined over L by its values at the generators of L as an K-algebra, i.e. by its values at $a_1, \dots, a_n$ (which can be related; think of the case of $\mathbb{Q}\left[i, j, \sqrt{3}\right]$ for example). If $L = K[a]$, it suffices to specify $\sigma(a)$ in order to completely

determine σ. For an element of the form $P(a)$ with $P \in K[X]$, we have $\sigma(P(a)) = P(\sigma(a))$.

6.3 Algebraic Elements and K-Homomorphisms

6.3.1 Proposition

Let K be a field, and let a be an algebraic element of finite degree n and minimal polynomial P over K.

1) *If L is an extension of K, if $a \in L$ and if $\sigma : L \to \mathbb{C}$ is a K-homomorphism, then $\sigma(a)$ is a conjugate of a over K. If L contains all the roots of a polynomial S in $K[X]$, then σ induces a permutation of the set of roots of S.*

2) *If b is a conjugate of a over K, there exists a unique K-isomorphism $\sigma : K[a] \to K[b]$ such that $\sigma(a) = b$.*

3) *The number of distinct K-homomorphisms from $K[a]$ to $\mathbb{C}$ is equal to n.*

PROOF. –

1) Let $P(X) = \sum_{0 \le k \le n} a_k X^k$ be the minimal polynomial of a over K. Because σ is a K-homomorphism and the coefficients of P lie in K, we have $\sigma(a_k) = a_k$ for $k = 0, \ldots, n$, so

$$P(\sigma(a)) = \sum_{0 \le k \le n} a_k (\sigma(a))^k = \sigma\left(\sum_{0 \le k \le n} a_k a^k\right) = \sigma(P(a)) = 0.$$

Thus $\sigma(a)$ is a conjugate of a over K.

Because σ is injective, the rest of the argument works by decomposing S into a product of irreducible factors.

2) Consider the diagram in Figure 6.1, where π denotes the canonical surjection, f and g are the homomorphisms defined by $f(X) = a$ and $g(X) = b$, and φ and ψ are their factorizations through π.

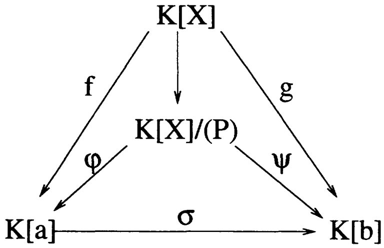


FIGURE 6.1.

Set $\sigma = \psi\phi^{-1}$. Like φ and ψ, it is a ring homomorphism (see §4.5.2); we have $\sigma f = \psi\varphi^{-1} f = \psi\pi = g$, so

$$\sigma(a) = \sigma f(X) = g(X) = b.$$

Thus, for every element x of K, we have $\sigma(x) = \sigma f(x) = g(x) = x$; this gives the result.

Let us show the uniqueness of σ. If σ' satisfies the same properties, then the restrictions of σf and $\sigma' f$ to K are the identity and $\sigma f(X) = b = \sigma' f(X)$; these two conditions imply that $\sigma f = \sigma' f$. As f is surjective, it follows that $\sigma = \sigma'$. An element of $K[a]$ of the form $\sum_{1\leq k\leq n} a_k a^k$ has image $\sum_{1\leq k\leq n} a_k b^k$.

3) Because P is irreducible of finite degree n, it has n distinct roots in $\mathbb{C}$. By part 2), each of these roots gives rise to a unique K-isomorphism from $K[a]$ to a subfield of $\mathbb{C}$. Then part 1) implies that there are no others. ◇

6.3.2 *Example*

The minimal polynomial X^3-2 of $\sqrt[3]{2}$ over $\mathbb{Q}$ has roots $\sqrt[3]{2}$, $j\sqrt[3]{2}$, and $j^2\sqrt[3]{2}$ in $\mathbb{C}$. Thus there exist three $\mathbb{Q}$-homomorphisms from $\mathbb{Q}[\sqrt[3]{2}]$ to $\mathbb{C}$ defined by the possible images of $\sqrt[3]{2}$ (Table 6.1).

	$\sqrt[3]{2}$
σ_1	$\sqrt[3]{2}$
σ_2	$j\sqrt[3]{2}$
σ_3	$j^2\sqrt[3]{2}$

TABLE 6.1.

The first one, σ_1, is the inclusion map; the other two, σ_2 and σ_3, can be expressed in the basis $\left\{1, \sqrt[3]{2}, \sqrt[3]{4}\right\}$ of $\mathbb{Q}\left[\sqrt[3]{2}\right]$ over $\mathbb{Q}$ by

$$\begin{aligned}\sigma_2\left(a + b\sqrt[3]{2} + c\sqrt[3]{4}\right) &= a + bj\sqrt[3]{2} + cj^2\sqrt[3]{4},\\ \sigma_3\left(a + b\sqrt[3]{2} + c\sqrt[3]{4}\right) &= a + bj^2\sqrt[3]{2} + cj\sqrt[3]{4},\end{aligned}$$

with a, b, c rational.

6.4 Extensions of Embeddings into $\mathbb{C}$

6.4.1 Definition

An *embedding* of a field L (contained in $\mathbb{C}$) into $\mathbb{C}$ is a homomorphism $\sigma : L \to \mathbb{C}$ of rings with unit.

If L is an extension of a field K, a K-homomorphism of L to $\mathbb{C}$ is an embedding. This generalization is useful for proving the corollary to Proposition 6.4.3 below.

6.4.2 Proposition

Let L be a field, and let $\sigma : L \to \mathbb{C}$ be a field embedding. Let a be an algebraic number of finite degree n over L. Then there are exactly n embeddings of $L[a]$ into $\mathbb{C}$ extending σ.

PROOF. – Let P denote the minimal polynomial of a over L. Consider the diagram in Figure 6.2, where

- i and j are the canonical inclusions;
- σ' is the homomorphism defined by $\sigma'(X) = X$ and $\sigma'|L = \sigma$;
- π and ρ are the canonical projections;
- σ'' is defined by passing to the quotient of σ';
- b is one of the n roots of $\sigma'(P)$ in $\mathbb{C}$;
- f and g are the homomorphisms defined by $f(X) = a$ and $g(X) = b$; fi and gj are the canonical inclusions;
- φ and ψ are the isomorphisms defined as in §4.5.2 (to see that ψ is an isomorphism, note that if $\sigma'(P)$ is reducible over $\sigma(L)$, i.e. if $\sigma'(P) = ST$ with S and T non-invertible, then $P = \sigma'^{-1}(ST) = \sigma'^{-1}(S)\sigma'^{-1}(T)$, which shows that $\sigma'^{-1}(S)$ or $\sigma'^{-1}(T)$ is invertible and consequently S or T is also invertible, which is a contradiction);

- $\tau = \psi\sigma''\varphi^{-1}$.

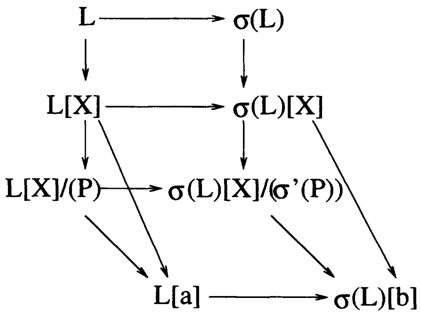


FIGURE 6.2.

Firstly, τ extends σ because $\tau fi = \psi\sigma''\varphi^{-1}fi = \psi\sigma''\pi i = gj\sigma$. If τ' is a second extension of σ to $L[a]$ such that $\tau'(a) = b$, we have $\tau' fi = gj\sigma = \tau fi$ and $\tau' f(X) = \tau'(a) = b = \tau f(X)$, which shows that $\tau' f = \tau f$, by the universal property of $L[X]$. Hence $\tau' = \tau$, since f is surjective. As $\tau(a)$ is necessarily one of the n roots of $\sigma'(P)$, since $\tau(P(a)) = \tau(f(P)) = \cdots = \sigma'(P)(\tau(a))$, the proposition is proved. ◇

The following formula can also be deduced from the proposition:

$$\tau\left(\sum_{0\leq k<n} x_k a^k\right) = \sum_{0\leq k<n} \sigma(x_k)b^k.$$

6.4.3 Proposition

Let L be a field, and let $M \subset \mathbb{C}$ be an extension of finite degree n of L. Let $\sigma : L \to \mathbb{C}$ be an embedding. The number of embeddings of M into $\mathbb{C}$ extending σ is equal to n.

PROOF. – We use induction on n. If $n = 1$, $M = L$ and the result follows. Assume $n > 1$. Figure 6.3 gives a diagram of the situation.

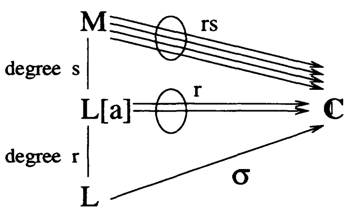


FIGURE 6.3.

Suppose that the property holds for every extension of finite degree strictly less than n, and let M be an extension (contained in $\mathbb{C}$) of finite degree n of L. Let a be an element of $M - L$; then a is algebraic over L of finite degree $r > 1$. The preceding proposition shows that there exist r extensions of σ to $L[a]$. If $M = L[a]$, we obtain the desired result; otherwise, by the induction hypothesis, since $s = [M : L[a]] < n$, we can assert that for each of the r extensions of σ to $L[a]$, there exist s extensions to M. The result then follows from the tower rule. ◇

COROLLARY. – *Let K be a field, and let $L \subset \mathbb{C}$ be an extension of finite degree n of K. There exist n K-homomorphisms from L to $\mathbb{C}$.*

PROOF. – It suffices to apply Proposition 6.4.3 to the embedding given by the inclusion of K into $\mathbb{C}$ (Figure 6.4). ◇

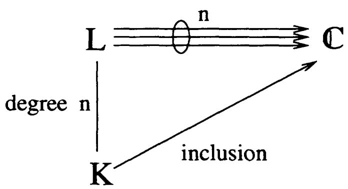


FIGURE 6.4.

6.5 The Primitive Element Theorem

6.5.1 Theorem and Definition

Let K be a field contained in $\mathbb{C}$, and let L be an extension of finite degree n of K. There exists an element a of L such that $L = K[a]$. Every element generating L is called a primitive element for the extension L of K.

COMMENTARY. – This result is due to Galois, who gave it without proof and deduced from it that the roots of a polynomial can be expressed rationally in terms of one particular element, using the following lemma:

"*Lemma II.* Given an arbitrary equation, which has no equal roots, whose roots are $a, b, c, \dots$, we can always form a function V of the roots, such that none of the values we obtain by permuting the roots in this function in every possible way are ever the same.

For example, we can take:

$$V = Aa + Bb + Cc + \cdots,$$

where $A, B, C, \ldots$ are suitably chosen integers."

A primitive element used to be called a *Galois resolvent.* The same term was also used for the minimal polynomial of such an element.

We prove the result here for subfields of $\mathbb{C}$; it generalizes not only to fields of characteristic 0 but even to all separable algebraic extensions of finite degree (defined in Chapter 15).

PROOF. – By §6.4.4, there exist n distinct K-homomorphisms from L to $\mathbb{C}$; let us denote them by $\sigma_1, \ldots, \sigma_n$. By the above lemma applied to the hyperplanes $\ker(\sigma_i - \sigma_j)$, $1 \leq i < j \leq n$, there exists an element a in L whose images under the $\sigma_1, \ldots, \sigma_n$ are all distinct. For $i = 1, \ldots, n$, $\sigma_i(a)$ is a conjugate of a over K, a is of degree $\geq n$ over K, so $[K[a] : K] = n$ and $L = K[a]$. ♢

LEMMA. – *Let V be a vector space over an infinite field k, and let $H_1, \ldots, H_r$ be a finite family of strict subspaces V. Then $V \neq \bigcup_{1 \leq i \leq r} H_i$.*

PROOF. – We use induction on r.

If $r = 1$, the result is clear. If $r > 1$, suppose the result holds for every family of $r - 1$ strict subspaces of V. Suppose that $V = \bigcup_{1 \leq i \leq r} H_i$; then by the induction hypothesis, there exists an element x in V which does not belong to $\bigcup_{1 \leq i \leq r-1} H_i$. So $x \in H_r$. On the other hand, let y be such that $y \notin H_r$, so $y \in \bigcup_{1 \leq i \leq r-1} H_i$. The set $E = \{x + \lambda y; \lambda \in k\}$ is infinite; thus there exists an integer i such that $1 \leq i \leq r$, and distinct elements λ and μ in k, such that $x + \lambda y \in H_i$ and $x + \mu y \in H_i$. We successively obtain $(\lambda - \mu)y \in H_i$, $y \in H_i$, $x \in H_i$, which contradicts the choices of x and y. ♢

6.5.2 Example

Consider the extension $L = \mathbb{Q}\left[\sqrt{2}, \sqrt{3}\right]$ of $\mathbb{Q}$. It is an extension of degree 4 of $\mathbb{Q}$. By §6.4.4, there are exactly four $\mathbb{Q}$-homomorphisms from L to $\mathbb{C}$. To construct them, we need to first construct the two $\mathbb{Q}$-homomorphisms $\tau_1, \tau_2 : \mathbb{Q}[\sqrt{2}] \to \mathbb{C}$ like in §6.3.1 2), associating to $\sqrt{2}$ one of its conjugates $\sqrt{2}$ or $-\sqrt{2}$, which leads to $\tau_1\left(\sqrt{2}\right) = \sqrt{2}, \tau_2\left(\sqrt{2}\right) = -\sqrt{2}$. Each of these two $\mathbb{Q}$-homomorphisms extends in two different ways, still by §6.3.1 2), to a $\mathbb{Q}$-homomorphism $\sigma_i : \mathbb{Q}\left[\sqrt{2}\right]\left[\sqrt{3}\right] \to \mathbb{C}$, $1 \leq i \leq 4$, by associating to $\sqrt{3}$ one of its conjugates $\pm\sqrt{3}$. The primitive elements of L are the elements whose images under these $\mathbb{Q}$-homomorphisms are all distinct; $\sqrt{2} + \sqrt{3}$, $\sqrt{2} + \sqrt{6}$, $m\sqrt{2} + n\sqrt{3}$ with m and n non-zero rational numbers, etc., are examples of such elements (Table 6.2).

	$\sqrt{2}$	$\sqrt{3}$	$\sqrt{2}+\sqrt{3}$	$\sqrt{2}+\sqrt{6}$
σ_1	$\sqrt{2}$	$\sqrt{3}$	$\sqrt{2}+\sqrt{3}$	$\sqrt{2}+\sqrt{6}$
σ_2	$\sqrt{2}$	$-\sqrt{3}$	$\sqrt{2}-\sqrt{3}$	$\sqrt{2}-\sqrt{6}$
σ_3	$-\sqrt{2}$	$\sqrt{3}$	$-\sqrt{2}+\sqrt{3}$	$-\sqrt{2}-\sqrt{6}$
σ_4	$-\sqrt{2}$	$-\sqrt{3}$	$-\sqrt{2}-\sqrt{3}$	$-\sqrt{2}+\sqrt{6}$

TABLE 6.2.

6.6 Linear Independence of K-Homomorphisms

The goal of this section is to state Dedekind's theorem (see §6.6.3). This theorem is a direct consequence of a theorem on characters.

6.6.1 Characters

DEFINITION. – A character of a group G into an arbitrary field K is a group homomorphism from G to the multiplicative group K^*.

Let $\chi : G \to K^*$ be a character. If e is the identity element of G, we have $\chi(e) = 1$; if g is of order n in G, then $\chi(g)^n = \chi(g^n) = 1$ shows that $\chi(g)$ is an n-th root of unity in K.

The characters of G are elements of the set F of set maps from G to K; we will say that characters are *linearly independent* if they are linearly independent in the K-vector space F.

6.6.2 Emil Artin's Theorem

Distinct characters of a group G into a field K are linearly independent.

PROOF. – Suppose there exist families of characters of G into K that are not linearly independent. Among all such families, choose a family $\chi_1, \dots, \chi_n$ such that n is minimal. Because n is minimal, there exist elements $\lambda_1, \dots, \lambda_n$ of K such that $\sum_{1\le i\le n} \lambda_i\chi_i = 0$ and such that none of the λ_i is zero. Of course, we have $n > 1$.

Because $\chi_1 \neq \chi_2$, there exists x in G such that $\chi_1(x) - \chi_2(x) \neq 0$. The linear combination $\sum_{1\le i\le n} \lambda_i\chi_i$ is zero, so for all y of G, we have

$$\sum_{1\le i\le n} \lambda_i\chi_i(y) = 0, \tag{6.1}$$

$$\sum_{1\le i\le n} \lambda_i\chi_i(xy) = \sum_{1\le i\le n} \lambda_i\chi_i(x)\chi_i(y) = 0. \tag{6.2}$$

Multiplying (1) by $\chi_1(x)$, we obtain

$$\sum_{1\leq i\leq n} \lambda_i\chi_1(x)\chi_i(y) = 0. \tag{6.3}$$

Subtracting (2) from (3), we have

$$\sum_{2\leq i\leq n} \lambda_i[\chi_1(x) - \chi_i(x)]\chi_i(y) = 0, \quad \text{so} \quad \sum_{2\leq i\leq n} \lambda_i[\chi_1(x) - \chi_i(x)]\chi_i = 0 \ \text{ in F.}$$

Because at least one of the coefficients is not zero, this equality contradicts the minimality of n. ◇

6.6.3 Corollary: Dedekind's Theorem

Let K be a field and $L \subset \mathbb{C}$ an extension of K. The K-homomorphisms from L to $\mathbb{C}$ form a set of linearly independent vectors in the $\mathbb{C}$-vector space of linear maps from L to $\mathbb{C}$.

PROOF. – The $\mathbb{C}$-vector space structure of the set of linear maps from L to $\mathbb{C}$ is induced by that of the $\mathbb{C}$-vector space of setwise maps from L to $\mathbb{C}$. Every K-homomorphism σ from L to $\mathbb{C}$ induces a character from the multiplicative group L^* to $\mathbb{C}$, since $\sigma(xy) = \sigma(x)\sigma(y)$; σ is a K-linear map since $\sigma(ax + by) = a\sigma(x) + b\sigma(y)$ for all x, y in L and all a, b in K. Thus, Theorem 6.2 applies. ◇

Exercises for Chapter 6

Exercise 6.1. K-homomorphisms

1) Determine $\mathbb{Q}$-automorphisms of the rings $\mathbb{Q}[7 + 3i]$ and $\mathbb{Q}[a]$ where a is a root of $X^2 + 52$.

2) Determine all the subfields of $\mathbb{C}$ that are $\mathbb{Q}$-isomorphic to $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt[3]{15}]$, to $\mathbb{Q}[\sqrt[5]{3}]$, to $\mathbb{Q}[\sqrt[6]{3}]$.

3) a) Determine the $\mathbb{Q}$-automorphisms of the rings $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt[4]{2}]$ and $\mathbb{Q}[\sqrt[8]{2}]$.

   b) Show that $\bigcup_{1\leq n} \mathbb{Q}[2^{1/n}]$ is an extension of $\mathbb{Q}$ (of infinite degree). Determine its $\mathbb{Q}$-automorphisms.

Exercise 6.2. Primitive elements

1) Let $K \subset \mathbb{C}$ be a field, and let a and b be two elements of K. Show that if $s = \sqrt{a} + \sqrt{b}$ (where $\sqrt{a}$ and $\sqrt{b}$ denote elements of $\mathbb{C}$ with squares a and b) is non-zero, then it is a primitive element of $K\left[\sqrt{a}, \sqrt{b}\right]$ over K.

2) Show that $j\sqrt{5}$ is a primitive element of $\mathbb{Q}\left[j, \sqrt{5}\right]$.

3) Show that $\sqrt[3]{2}+\sqrt{2}$ is a primitive element of the extension $\mathbb{Q}\left[\sqrt[3]{2}, \sqrt{2}\right]$ of $\mathbb{Q}$. Give other primitive elements for this extension.

4) Determine a primitive element of $\mathbb{Q}[a, j]$, where a is a root of $X^3 - X + 1$.

5) Let K be a field, and let a and b be algebraic elements over K. Show that there exists an integer r in $\mathbb{Z}$ such that $a + rb$ is a primitive element of $L = K[a, b]$ over K. Generalize.

Exercise 6.3. K-endomorphisms of an algebraic extension

Let L be an algebraic extension of a field K of finite or infinite degree, and let $\sigma : L \to L$ be a K-homomorphism. Let a be an element of L, P its minimal polynomial over K, and A the set of roots of P in L.

1) Show that $\sigma(A) = A$.

2) Deduce that σ is a K-isomorphism.

Solutions to Some of the Exercises

Solution to Exercise 6.1.

1) As $\mathbb{Q}[7+3i] = \mathbb{Q}[i]$, there are two $\mathbb{Q}$-automorphisms of $\mathbb{Q}[7+3i]$, namely the identity and the one induced by complex conjugation.

As $\mathbb{Q}[a] = \mathbb{Q}[i\sqrt{13}]$, there are two $\mathbb{Q}$-automorphisms of $\mathbb{Q}[a]$, defined by $\sigma(a) = \pm i\sqrt{13}$; namely the identity and the one induced by complex conjugation.

2) The only field that is $\mathbb{Q}$-isomorphic to $\mathbb{Q}[\sqrt{3}]$ is itself, although $\sqrt{3}$ has two conjugates over $\mathbb{Q}$.

Over $\mathbb{Q}$, $\sqrt[3]{15}$ is a conjugate of itself, of $j\sqrt[3]{15}$, and of $j^2\sqrt[3]{15}$. Thus the field $\mathbb{Q}[\sqrt[3]{15}]$ is $\mathbb{Q}$-isomorphic to $\mathbb{Q}[\sqrt[3]{15}]$, $\mathbb{Q}[j\sqrt[3]{15}]$, and $\mathbb{Q}[j^2\sqrt[3]{15}]$. These three fields are distinct; the first one is contained in $\mathbb{R}$, unlike the other two, and if $\mathbb{Q}[j\sqrt[3]{15}] = \mathbb{Q}[j^2\sqrt[3]{15}]$, then the element j, which is the quotient

of the two generators and is quadratic over $\mathbb{Q}$, would belong to a cubic extension.

Because the polynomial $X^5 + 3$ is irreducible over $\mathbb{Q}$, $\sqrt[5]{3}$ has five conjugates over $\mathbb{Q}$ and $\mathbb{Q}[\sqrt[5]{3}]$ is $\mathbb{Q}$-isomorphic to the five fields $\mathbb{Q}[\sqrt[5]{3}]$, $\mathbb{Q}[\zeta\sqrt[5]{3}]$, $\mathbb{Q}[\zeta^2\sqrt[5]{3}]$, $\mathbb{Q}[\zeta^3\sqrt[5]{3}]$, $\mathbb{Q}[\zeta^4\sqrt[5]{3}]$, where $\zeta = e^{2i\pi/5}$. These five fields are all distinct, since the equality of two of them would imply that one of the $\zeta^k, 1 \leq k \leq 4$, which are of degree 4 over $\mathbb{Q}$, would belong to it, even though the extensions are of degree 5.

As $\sqrt[6]{3}$ has six conjugates over $\mathbb{Q} : \pm\sqrt[6]{3}$, $\pm j\sqrt[6]{3}$, $\pm j^2\sqrt[6]{3}$, the field $\mathbb{Q}[\sqrt[6]{3}]$ is $\mathbb{Q}$-isomorphic to one of the three fields $\mathbb{Q}[\sqrt[6]{3}]$, $\mathbb{Q}[j\sqrt[6]{3}]$ or $\mathbb{Q}[j^2\sqrt[6]{3}]$.

Let us show that these three fields are all distinct. The first one is contained in $\mathbb{R}$, and the other two are not. The two last ones are of degree 6 over $\mathbb{Q}$. If they were equal, then j would belong to $\mathbb{Q}[j\sqrt[6]{3}]$, and consequently $\mathbb{Q}[j\sqrt[6]{3}] = \mathbb{Q}[j, \sqrt[6]{3}]$. But the last field is of degree 12 over $\mathbb{Q}$.

3) a) The only $\mathbb{Q}$-automorphisms of $\mathbb{Q}[\sqrt{2}]$, of $\mathbb{Q}[\sqrt[4]{2}]$, and of $\mathbb{Q}[\sqrt[8]{2}]$ are defined by $\sigma(\sqrt{2}) = \pm\sqrt{2}$, $\sigma(\sqrt[4]{2}) = \pm\sqrt[4]{2}$, $\sigma(\sqrt[8]{2}) = \pm\sqrt[8]{2}$.

b) Let x and y lie in $\cup_{1\leq n}\mathbb{Q}[2^{1/n}]$. There exist integers r and s such that $x \in \mathbb{Q}[2^{1/r}]$ and $y \in \mathbb{Q}[2^{1/s}]$; we see that x and y lie in the field $\mathbb{Q}[2^{1/rs}]$, and we easily deduce that $\cup_{1\leq n}\mathbb{Q}[2^{1/n}]$ is a field.

Let σ be a $\mathbb{Q}$-automorphism of $\cup_{1\leq n}\mathbb{Q}[2^{1/n}]$. We have $\sigma(2^{1/n}) = \pm 2^{1/n}$. As $\sigma(2^{1/n}) = \sigma[(2^{1/2n})^2] > 0$ for every integer n, we have $\sigma(2^{1/n}) = 2^{1/n}$ and $\sigma =$id. This result does not tell us anything about the extension, but we are in the case of an extension from which the conjugates of $\sqrt[4]{2}$, $\sqrt[8]{2}$, etc., are absent.

Solution to Exercise 6.2.

1) This follows from $\sqrt{a} = (s/2)+(a-b)/(2s)$ and $\sqrt{b} = (s/2)-(a-b)/(2s)$.

2) Set $a = j\sqrt{5}$. We have $\sqrt{5} = a^3/5$ and $j = a^4/25$. The result follows.

3) We know that $[\mathbb{Q}[\sqrt[3]{2}, \sqrt{2}] : \mathbb{Q}] = 6$. An element of $\mathbb{Q}\left[\sqrt[3]{2}, \sqrt{2}\right]$ is primitive if its images under the six $\mathbb{Q}$-homomorphisms from $\mathbb{Q}\left[\sqrt[3]{2}, \sqrt{2}\right]$ to $\mathbb{C}$ are distinct. The image of $\sqrt[3]{2}$ under one of these six $\mathbb{Q}$-homomorphisms is $\sqrt[3]{2}$, $j\sqrt[3]{2}$, $j^2\sqrt[3]{2}$ and the image of $\sqrt{2}$ is $\pm\sqrt{2}$. The element $\sqrt[3]{2} + \sqrt{2}$ is thus primitive, as are the elements of the form $x\sqrt[3]{2} + y\sqrt{2}$ for x and y nonzero rational numbers (two of the images are real and obviously distinct, and the other four are non-real with distinct real or imaginary parts. To visualize them, draw a regular hexagon, place each of the six numbers at a vertex and draw a line directly between two vertices if we have shown that they correspond to distinct numbers. To conclude, every pair of vertices must be connected by a line.)

A simpler primitive element is $2^{1/6}$.

4) Set $b = a + j$. The condition $(b - j)^3 - b + j + 1 = 0$ shows that $\mathbb{Q}[j] \subset \mathbb{Q}[b]$, so $\mathbb{Q}[b] = \mathbb{Q}[a, j]$.

5) Set $n = [L : K]$. There exist distinct n K-homomorphisms from L to $\mathbb{C}$; we denote them by $\sigma_1, \ldots, \sigma_n$. If there did not exist $r \in \mathbb{Z}$ such that $a + rb$ has distinct images under these n K-homomorphisms, then for every r there would exist distinct integers i and j with $1 \leq i, j \leq n$ such that $\sigma_i(a + rb) = \sigma_j(a + rb)$. As r can take an infinity of values, and the pairs (i, j) only have a finite number of values, there would exist distinct integers r and s, and distinct integers i and j, such that $\sigma_i(a + rb) = \sigma_j(a + rb)$ and $\sigma_i(a + sb) = \sigma_j(a + sb)$. Taking the difference and simplifying by $r - s$, we obtain $\sigma_i(b) = \sigma_j(b)$ then $\sigma_i(a) = \sigma_j(a)$, which would imply that $\sigma_i = \sigma_j$, a contradiction.

It follows that if $L = K[a_1, \ldots, a_n]$, there exist integers $r_1, \ldots, r_n$ such that $\sum_{1 \leq i \leq n} r_i a_i$ is a primitive element of L over K.

Solution to Exercise 6.3.

1) We know that σ is injective. As $\sigma(A) \subset A$ and A is finite, we have $\sigma(A) = A$.

2) By **1)**, a lies in the image of σ; consequently, σ is surjective, which gives the result.

7
Normal Extensions

7.1 Splitting Fields

7.1.1 Definition

Let K be a subfield of $\mathbb{C}$, and let P be a polynomial of degree n in $K[X]$. Let $x_1, \ldots, x_n$ be the (not necessarily distinct) roots of P in $\mathbb{C}$. The field $K[x_1, \ldots, x_n]$, which by §4.6.2 is an extension of K of finite degree, is called the *splitting field* of P over K.

Let P be a polynomial. Note that the polynomial $P_1 = P/\gcd(P, P')$ has the same roots as P, but all as simple roots. Thus, in characteristic 0, the splitting field of P is the same as that of P_1, since the splitting field is obtained by adjoining the roots. Thus, we can restrict our attention to polynomials with distinct roots.

REMARK. – We saw in §4.7 how to construct an extension of a field K containing a root of a polynomial P irreducible over K; we called such an extension a *rupture field* for P.

EXAMPLE. – The splitting field of $X^3 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}[j, \sqrt[3]{2}]$ since the roots of $X^3 - 2$ are $\sqrt[3]{2}$, $j\sqrt[3]{2}$, and $j^2\sqrt[3]{2}$. It is an extension of degree 6 of $\mathbb{Q}$. The rupture fields of $X^3 - 2$ over $\mathbb{Q}$ contained in $\mathbb{C}$ are $\mathbb{Q}[\sqrt[3]{2}]$, $\mathbb{Q}[j\sqrt[3]{2}]$, and $\mathbb{Q}[j^2\sqrt[3]{2}]$.

7.1.2 Splitting Field of a Cubic Polynomial

PROPOSITION. – *Let K be a field contained in $\mathbb{C}$ and $P(X) = X^3 + pX + q$ an irreducible cubic polynomial in $K[X]$. Let a, b, and c denote the roots of P in $\mathbb{C}$ and $d = (a-b)(b-c)(c-a)$.*

The splitting field of P over K is $K[a,d]$. It is of degree 3 or 6 over K according to whether the discriminant $D(P) = -4p^3 - 27q^2$ of P is or is not a square in K.

PROOF. – The splitting field of P over K is $K[a,b,c]$, and the inclusion $K[a,d] \subset K[a,b,c]$ is clear.

Conversely, we know that $d^2 = D(P) \neq 0$ and $a \neq 0$. The equality

$$(a-b)(c-a) = a(b+c) - a^2 - bc = -2a^2 + \frac{q}{a}$$

shows that $b - c = d/\left((a-b)(c-a)\right)$ lies in $K[a,d]$. As $b+c = -a$ also lies in $K[a,d]$, b, c both lie in $K[a,d]$ and we have $K[a,d] = K[a,b,c]$.

Now, $K[a]$ and $K[d]$ are intermediate extensions between $K[a,d]$ and K, but $[K[a] : K] = 3$ and $[K[d] : K]$ is equal to either 1 or 2 according to whether $d \in K$ or $d \notin K$; this suffices for the proof. ♢

REMARK. – If a cubic polynomial is not irreducible over K, its splitting field can be of degree 1 or 2 over K.

7.2 Normal Extensions

DEFINITION. – A *normal extension* of a field K (either contained in $\mathbb{C}$ or not) is an algebraic extension N of K (of finite or infinite degree) such that every irreducible polynomial in $K[X]$ having a root in N has all its roots in N. In other words, all conjugates of elements of N must lie in N.

We will try as much as possible to reserve the letter K for the base field, the letters $L, L', \ldots$ for arbitrary extensions of K, and $N, N', \ldots$ for normal extensions K.

EXAMPLES. –

a) By Proposition 7.4.1 below, a splitting field is a normal extension of finite degree.

b) The intersection of normal extensions is normal.

c) A normal extension N of a field K is also a normal extension of every intermediate extension L between K and N (see Proposition 7.5 below).

COMMENTARY. – In the case of infinite fields of non-zero characteristic, it is necessary to distinguish between "normal extensions" and Galois extensions

(see Chapter 15). In characteristic 0, the two notions are equivalent; we use the the expression "normal extension".

7.3 Normal Extensions and K-Homomorphisms

PROPOSITION. – *An algebraic extension $N \subset \mathbb{C}$ of finite degree of a field K is normal if and only if the image of every K-homomorphism $\sigma : N \to \mathbb{C}$ is contained in N.*

PROOF. – If N is a normal extension of K, then for every x in N and every K-homomorphism $\sigma : N \to \mathbb{C}$, x is algebraic over K, and by §4.3.1, $\sigma(x)$ is a conjugate of x. Consequently, $\sigma(x)$ lies in N, so that $\sigma(N) \subset N$. Moreover, σ is a K-automorphism of N by §6.2.2.

Conversely (Figure 7.1), if an element x of N has minimal polynomial P over K, and if y is a root of P in $\mathbb{C}$, then by §6.3.1, there exists a K-homomorphism $\sigma : K[x] \to \mathbb{C}$ such that $\sigma(x) = y$. By §6.4.3, this homomorphism extends to a K-homomorphism $\sigma' : N \to \mathbb{C}$. But as $\sigma'(N) \subset N$ and $\sigma'(x) = y$, y is an element of N.

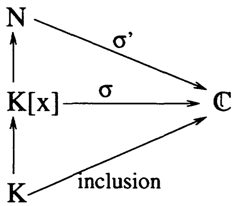


FIGURE 7.1.

7.4 Splitting Fields and Normal Extensions

In this section, we give the precise relation between a splitting field and a normal extension of finite degree.

7.4.1 Proposition

Let $K \subset \mathbb{C}$ be a field. Let P be a polynomial in $K[X]$ of degree n, and let N be the splitting field of P over K. Then

1) N is a normal extension of finite degree of K.

2) $[N : K]$ divides $n!$.

PROOF. –

1) Let $x_1, \ldots, x_n$ be the (not necessarily distinct) roots of P in $\mathbb{C}$. We know that $N = K[x_1, \ldots, x_n]$ is an algebraic extension of K.

   Let $\sigma : N \to \mathbb{C}$ be a K-homomorphism. For $i = 1, \ldots, n$, we have $0 = \sigma(P(x_i)) = P(\sigma(x_i))$, so $\sigma(x_i) \in \{x_1, \ldots, x_n\} \subset N$. As $\{x_1, \ldots, x_n\}$ generates N, we have $\sigma(N) \subset N$ and Proposition 7.3 concludes the proof.

2) We use induction on n. For $n = 1$, the result is obvious. Suppose now that $n > 1$. If P is irreducible and x is a root of P in N, we have $[K[x] : K] = n$, and by the induction hypothesis, $[N : K[x]]$ divides $(n-1)!$, where N is the splitting field of $P/(X - x)$ over $K[x]$. This gives the result. If P has an irreducible factor S of degree k, then $n > k \geq 1$, and if N' is the splitting field of S over K, then $[N' : K]$ divides $k!$ and $[N : N']$ divides $(n-k)!$, where N is the splitting field of P/S over N. Consequently, $[N : K]$ divides $k!(n-k)!$, so it divides $n!$. ♢

7.4.2 Converse

Let $N \subset \mathbb{C}$ be a normal extension of finite degree of a field K. Then N is the splitting field over K of an irreducible polynomial P in $K[X]$ of degree $[N : K]$.

PROOF. – Because N is an extension of finite degree of K, the Primitive Element Theorem (§6.5) shows that there exists an element x in N such that $N = K[x]$. The minimal polynomial P of x over K is of degree $[N : K]$. It is irreducible, so all of its roots are in N since N is a normal extension of K. The splitting field of P over K is thus N. ♢

7.5 Normal Extensions and Intermediate Extensions

PROPOSITION. – *Let N be a normal extension of finite degree of a field K. Then N is a normal extension of every intermediate extension L between K and N.*

PROOF. – As $[N : K]$ is finite, $[N : L]$ is finite. By §7.4.2, N is the splitting field over K of a polynomial P in $K[X]$. If $x_1, \ldots, x_n$ are the roots of P in $\mathbb{C}$, we have $N = K[x_1, \ldots, x_n]$; as $K \subset L \subset N$, we have $N = L[x_1, \ldots, x_n]$, which shows that N is the splitting field of P over L, where P is considered as a polynomial in $L[X]$. By §7.4.1, this gives the result. ♢

REMARK. – The above property can be recalled by the diagram in Figure 7.2. The example of Figure 7.3 shows that conversely, L may or may not be a normal extension of K.

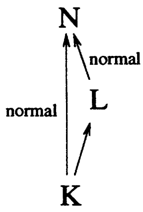


FIGURE 7.2.

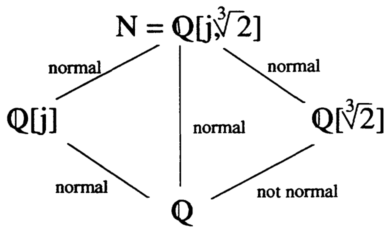


FIGURE 7.3.

7.6 Normal Closure

7.6.1 Definition

Let K be a field, and let $L \subset \mathbb{C}$ be an algebraic extension of K. The *normal closure* of L over K in $\mathbb{C}$ is the smallest normal extension N of K containing L. This extension always exists; it is the intersection of the set of normal extensions of K containing L, a set which is non-empty since $\mathbb{C}$ is a normal extension of all its subfields.

7.6.2 Proposition

Let $K \subset \mathbb{C}$ be a field. The normal closure in $\mathbb{C}$ of a finite degree extension $L \subset \mathbb{C}$ of K is a finite degree extension of K. It is the splitting field of the minimal polynomial of a primitive element of L over K.

PROOF. – By the Primitive Element Theorem, there exists an element a of L such that $L = K[a]$. Let P be the minimal polynomial of a over K and let N be the splitting field of P over K. N is a normal extension of finite degree of K, which contains L; moreover, every normal extension of K containing L contains all the roots P, so it contains N. The normal closure of K in $\mathbb{C}$ is thus N. ◊

7.6.3 Proposition

Let $K \subset \mathbb{C}$ be a field, and let $L = K[a_1, \ldots, a_n] \subset \mathbb{C}$ be a finite degree extension of K. The normal closure N of L over K inside $\mathbb{C}$ is the extension of K by the set of conjugates over K of the elements $a_1, \ldots, a_n$.

PROOF. – Let A be the set of conjugates over K of the elements $a_1, \ldots, a_n$. Because N is a normal extension of K, we have $N \supset A$, so $N \supset K[A]$.

As $K[A]$ is the splitting field of the product of the minimal polynomials of $a_1, \ldots, a_n$ over K, it is a normal extension of K. Thus $N = K[A]$. ♢

7.7 Splitting Fields: General Case

Let us now consider arbitrary fields instead of only subfields of $\mathbb{C}$. Let K be an arbitrary field, and P an irreducible polynomial of degree n in $K[X]$. We know that P has no roots in K. In §4.7, we saw how to construct an extension of K containing a root of P. Let us now indicate how to construct an extension N of K which is a splitting field of P over K, i.e. a field which contains all the roots of P and is generated by them.

PROPOSITION. (**Kronecker**) – *Let K be an arbitrary field, and let P be a polynomial of degree n in $K[X]$.*

1) *There exists an extension N of K which is a splitting field for P over K.*

2) *$[N : K]$ divides $n!$.*

3) *Two splitting fields N and N' of P over K are K-isomorphic. If the roots of P are simple in N and N' (we say that P is separable), then the number of K-isomorphisms from N to N' is equal to $[N : K]$.*

PROOF. –

1) We use induction on n. If $n \leq 1$, then $N = K$ works.

   If $n > 1$, factor P as a product of irreducible factors over K. If all these factors are of degree 1, then again $N = K$ works. Otherwise, let S be an irreducible factor of degree > 1 of P. Set $L = K[X]/(S)$ and let x denote the class of X in L. L is a field and in $L[X]$, we can factor P in the form $(X - x)T$ with $T \in L[X]$. By the induction hypothesis, there exists a field N which is a splitting field of T over L. This field is a splitting field of P over K.

2) See the proof of §7.4.1 2).

3) LEMMA. *Let $\sigma : K \to K'$ be a field isomorphism and N' a splitting field of $\sigma(P)$ over K'. We can extend σ to a homomorphism $\tau : N \to N'$. If the roots of P are simple, the number of extensions is equal to $[N : K]$.*

   To prove the lemma, we use induction on $[N : K]$. If $[N : K] = 1$, then P factors as a product of linear factors in $K[X]$ and everything is clear. If $[N : K] > 1$, let S be an irreducible factor of degree > 1 of P. Let x be a root of S in N, and set $L = K[x]$. Let x' be a

root of $\sigma(S)$ in N', and set $L' = K'[x']$. As in §6.4.2, we construct the isomorphisms $L \simeq K[X]/(S) \simeq K'[X]/(\sigma(S)) \simeq L'$ which define the isomorphism $\sigma_1 : L \to L'$ with $\sigma_1(x) = x'$. By the induction hypothesis, this σ_1 extends to a homomorphism $\tau : N \to N'$. If the roots of P are simple, the number of such extensions σ_1 is equal to the number of roots of $\sigma(S)$ in N', i.e. to $\deg(\sigma(S)) = [L : K]$. The induction hypothesis then gives the desired number.

To finish the proof, we use the lemma to extend $\mathrm{id}(K)$, obtaining a (necessarily injective) homomorphism $\tau : N \to N'$, proving that $[N : K] \leq [N' : K]$. Inverting the roles of N and N', we have $[N' : K] \leq [N : K]$, so τ is an isomorphism. ◇

Toward Chapter 8

Chapters 4, 6, and 7 suffice to open the doors of the "paradise" created (discovered?) by Galois; Chapter 8 will describe the heart of his theory, the Galois correspondence.

Exercises for Chapter 7

Exercise 7.1. Splitting fields

1) Determine the splitting field of $aX^2 + bX + c$ with $a \neq 0$ over $K = \mathbb{Q}(a, b, c)$.

2) Determine the splitting fields of the following polynomials by determining the degrees of the corresponding extensions of $\mathbb{Q}$:

a) $X^3 - 1$;

b) $X^6 - 1$;

c) $X^4 - 7$;

d) $X^3 - X^2 - X - 2$;

e) $X^6 - 10X^4 + 31X^2 - 30$;

f) $X^5 + X^4 + X^3 + X^2 + X + 1$;

g) $X^4 + 1$.

Exercise 7.2. Normal extensions

1) Show that a quadratic extension of a field K is necessarily normal.

2) Does the fact that $\sqrt[3]{2}$ is an element of $\mathbb{Q}[\sqrt[3]{2}]$ whereas $j\sqrt[3]{2}$ and $j^2\sqrt[3]{2}$ are not imply that $\mathbb{Q}[\sqrt[3]{2}]$ is not a normal extension of itself?

3) Let N be a normal extension of a field L. Is it a normal extension of every subfield K of L? Consider in particular the example $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\sqrt[4]{2}]$; give the normal closure of the extension $\mathbb{Q}[\sqrt[4]{2}]$ of $\mathbb{Q}$.

4) Determine the normal extensions of $\mathbb{Q}$ generated by $\sqrt{3}+\sqrt{2}$, $\sqrt{3}+i$, $\sqrt[3]{2}+\sqrt{2}$, $\sin\frac{2\pi}{5}$, $\zeta = e^{2i\pi/n}$ for integers n.

5) Let $N \subset \mathbb{C}$ be a normal extension of finite degree of a field K, and let L be an extension of K and $N' \subset \mathbb{C}$ the extension of K generated by $L \cup N$. Show that N' is a normal extension of L.

Exercise 7.3. Cubic normal extensions

1) Let K be a field contained in $\mathbb{C}$, and let P be an irreducible cubic polynomial in $K[X]$ of discriminant $D = d^2$, $d \in \mathbb{C}$. Let a be a root of P in $\mathbb{C}$. Show that $K[a]$ is a normal extension of K if and only if d lies in K.

2) Let a, b, c be the roots of $X^3 - 3X + 1$ in $\mathbb{C}$.

   a) Show that $\mathbb{Q}[a]$ is a normal extension of $\mathbb{Q}$.

   b) Express b and c in the basis $\{1, a, a^2\}$.

Exercise 7.4. Proof of d'Alembert's theorem (fundamental theorem of algebra)

In this problem, we will show that every non-constant polynomial P in $\mathbb{C}[X]$ has at least one root in $\mathbb{C}$, following an idea due to Pierre Samuel (see the bibliography).

1) Show that it is enough to consider polynomials with real coefficients (consider $P\overline{P}$).

   Now assume that P has real coefficients; we will proceed by induction on $r = v_2(\deg(P))$, where $v_2(n)$ is the largest power of 2 dividing n.

2) Show the result in the case $r = 0$, then in the case $\deg(P) = 2$.

3) Now suppose $r \geq 1$. Take a splitting field of P. Note that we cannot assume that this splitting field is contained in $\mathbb{C}$ (since that is

a consequence of the theorem we are now proving), so we need to construct the splitting field by successive quotients as in §7.7. For $1 \le i \le n = \deg(P)$, let a_i denote the roots of P in this splitting field.

For every real number c, set

$$Q_c(X) = \prod_{1 \le i < j \le n} (X - a_i - a_j - c a_i a_j).$$

a) Determine $v_2(\deg(Q_c))$.

b) Show that the coefficients of Q_c are real.

c) Finish the proof.

Solutions to Some of the Exercises

Solution to Exercise 7.1.

1) According to whether the discriminant $b^2 - 4ac$ is or is not a square in K, the splitting field of $aX^2 + bX + c$ is either K or the quadratic extension of K generated by a root of $b^2 - 4ac$.

2) a), b), d), and **f).** $\mathbb{Q}[j]$ is the splitting field in these four cases, since we have

$$X^3 - 1 = (X-1)(X^2+X+1),$$
$$X^6 - 1 = (X-1)(X^2+X+1)(X+1)(X^2-X+1),$$
$$X^3 - X^2 - X - 2 = (X-2)(X^2+X+1),$$
$$X^5+X^4+X^3+X^2+X+1 = \frac{X^6-1}{X-1} = (X^2+X+1)(X+1)(X^2-X+1).$$

c) The polynomial $X^4 - 7$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion, and its splitting field is $\mathbb{Q}[\pm\sqrt[4]{7}, \pm i\sqrt[4]{7}] = \mathbb{Q}[i, \sqrt[4]{7}]$. This is an extension of degree 8 over $\mathbb{Q}$.

e) The polynomial factors as $(X^2-2)(X^2-3)(X^2-5)$; its splitting field is $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$, which is of degree 8 over $\mathbb{Q}$ by Exercise 4.5 6).

g) Set $\zeta = e^{i\pi/4} = (1+i)/\sqrt{2})$. The splitting field N of X^4+1 over $\mathbb{Q}$ is $\mathbb{Q}[\zeta, \zeta^3, \zeta^5, \zeta^7] = \mathbb{Q}[\zeta]$; it contains $i = \zeta^2$, so it contains $\sqrt{2}$, so that $N = \mathbb{Q}[i, \sqrt{2}]$.

Solution to Exercise 7.2.

1) Let L be a quadratic extension of K. Then we must have $L = K[x]$ for every x in L which is not in K, since they are all of degree 2 over K.

Let y be the second root of the minimal polynomial of x over K. Because $x+y \in K$, we have $L = K[x,y]$, so L is a splitting field.

2) No: $\sqrt[3]{2}$ is a root of the polynomial $X - \sqrt[3]{2}$ of $\mathbb{Q}[\sqrt[3]{2}][X]$.

3) This result is false in general, since a field is always a normal extension of itself, but is not always a normal extension of its subfields.

A false argument: let P be an irreducible polynomial of $K[X]$ having a root in N. As a polynomial in $L[X]$, it has a root in N, so all its roots must lie in N. Thus N is a normal extension of K.

The error in this reasoning is that in fact, P may no longer be irreducible over L. For example, take $K = \mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] = L \subset \mathbb{Q}[\sqrt[4]{2}] = N$ and $P(X) = X^4 - 2$. Then P is irreducible over $\mathbb{Q}$, but not over $\mathbb{Q}[\sqrt{2}]$ since $X^4 - 2 = (X^2 - \sqrt{2})(X^2 + \sqrt{2})$ and the second factor has no roots in N. The normal closure of the extension $\mathbb{Q}[\sqrt[4]{2}]$ of $\mathbb{Q}$ is $\mathbb{Q}[i, \sqrt[4]{2}]$.

4) We already saw that $\mathbb{Q}[\sqrt{3}+\sqrt{2}] = \mathbb{Q}[\sqrt{3},\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}+i] = \mathbb{Q}[\sqrt{3},i]$ and $\mathbb{Q}[\sqrt[3]{2}+\sqrt{2}] = \mathbb{Q}[\sqrt[3]{2},\sqrt{2}]$ (Exercise 4.2). Thus $\mathbb{Q}[\sqrt{3}+\sqrt{2}]$ and $\mathbb{Q}[\sqrt{3}+i]$ are normal extensions, since they are the splitting fields of $(X^2-2)(X^2-3)$ and $(X^2+1)(X^2-3)$, and $\sqrt[3]{2}+\sqrt{2}$ generates the normal extension $N = \mathbb{Q}[\sqrt[3]{2}, j, \sqrt{2}]$, which is the splitting field of $(X^2-2)(X^3-2)$, of degree 12 over $\mathbb{Q}$.

We saw in Exercise 4.5 that $a = 4\sin\frac{2\pi}{5} = \sqrt{10+2\sqrt{5}}$ and that the minimal polynomial of a over $\mathbb{Q}$ is $X^4 - 20X^2 + 80$. The conjugates of a over $\mathbb{Q}$ are thus $\pm\sqrt{10 \pm 2\sqrt{5}}$. Now, $\sqrt{10-2\sqrt{5}} = 4\sqrt{5}/\sqrt{10+2\sqrt{5}}$ belongs to $\mathbb{Q}[\sin(2\pi/5)]$ since $\sqrt{5} = (a^2-10)/2$ belongs to it. Thus, $\mathbb{Q}[\sin(2\pi/5)]$ is a normal extension of $\mathbb{Q}$.

Finally, in the case $\zeta = e^{2i\pi/n}$ for an integer n, $\mathbb{Q}[\zeta]$ is the splitting field of $X^n - 1$ over $\mathbb{Q}$, so it is a normal extension of $\mathbb{Q}$.

5) By the Primitive Element Theorem, we know that N is the splitting field of a polynomial P in $K[X]$; then N' is the splitting field of the polynomial P over L.

Solution to Exercise 7.3.

1) $K[a]$ is a normal extension of K if and only if $K[a] = K[a,d]$, since $K[a,d]$ is the splitting field of P over K (§7.1.2); this condition is equivalent to $d \in K[a]$, so $d \in K$, since d is of degree 1 or 2 over K.

2) a) As $X^3 - 3X + 1$ has no rational root, it is an irreducible polynomial; its discriminant is 81, which is a square in $\mathbb{Q}$. Thus $[\mathbb{Q}[a] : \mathbb{Q}] = 3$ and $\mathbb{Q}[a]$ is a normal extension of K.

b) We use the computations of §7.1.2. On the one hand, we have

$$b + c = -a.$$

On the other, we have

$$b - c = \frac{d}{(a-b)(c-a)} = \frac{d}{-2a^2 + \dfrac{1}{a}}.$$

Take $d = 9$ (the other possible choice, -9, simply ends up exchanging the roles of b and c). Using the techniques of Chapter 4 (the method of indeterminate coefficients or Bézout's identity), we find $b - c = 4 - a - 2a^2$, which gives $b = 2 - a - a^2$ and $c = a^2 - 2$.

8
Galois Groups

In this chapter, we reach the very heart of Galois theory. To every polynomial with coefficients in a field K, with splitting field N over K, we associate a group G called its *Galois group*. We show that the subgroups of G are in bijective correspondence with the intermediate extensions between N and K. This correspondence makes it possible to solve problems about polynomials and their splitting fields algebraically, by computing groups. Over the following chapters, we sketch out this dictionary between the properties of an equation and the algebraic properties of its associated group.

8.1 Galois Groups

8.1.1 The Galois Group of an Extension

DEFINITION. – Let K be a field, and let L be an extension of K. The set of K-automorphisms of L is equipped with a group structure whose group law is the composition of K-automorphisms. We will denote this group by $\mathrm{Gal}(L|K)$, and call it the *Galois group of the extension L over K.*

Throughout most of this text, we will consider Galois groups of normal extensions of finite degree; non-normal extensions L of K do not possess enough K-automorphisms to make the fundamental theorem of the Galois correspondence (see §8.5 below) work.

8.1.2 The Order of the Galois Group of a Normal Extension of Finite Degree

PROPOSITION. –*Let N be a normal extension of finite degree of a field K contained in $\mathbb{C}$. Then the order of the group* $\mathrm{Gal}(N|K)$ *is equal to* $[N : K]$.

PROOF. – By §6.4.4, there exist $[N : K]$ K-homomorphisms from N to $\mathbb{C}$. By §7.3, their image lies in N; thus these homomorphisms are actually K-automorphisms (§6.2.2). ♢

8.1.3 The Galois Group of a Polynomial

Let K be a field, and let P be a polynomial of degree n in $K[X]$ such that P has distinct roots. If $K \subset \mathbb{C}$, recall that we can always replace P by a polynomial having the same roots as P, but as simple roots. More generally, if K is of characteristic 0, we can replace P by the greatest common divisor of P and its derivative P'; this method was first suggested by Johann Hudde in 1657 (see the book by J.-P. Tignol). Let E be the set of roots of P in $\mathbb{C}$, and let $N = K[E]$ be the splitting field of P over K. We know that N is a finite degree extension of K, which is normal by Proposition 7.4.1. The Galois group $G = \mathrm{Gal}(N|K)$ is also called the *Galois group of the polynomial P over K.*

8.1.4 The Galois Group as a Subgroup of a Permutation Group

In Exercise 8.1, we recall the definition and some properties of group actions on sets.

PROPOSITION. – *1) With the notation of §8.1.3, G acts on E. This action makes it possible to identify G with a subgroup of the group S_E of permutations of E, and with mutually conjugate subgroups of the group S_n of permutations of $\{1, \dots, n\}$.*

2) The order of G divides $n!$.

3) If P is irreducible, the action of G on E is transitive.

PROOF. – 1) Let $\sigma \in G$. For every $x \in E$, $\sigma(x)$ lies in E, since it is a conjugate of x (§6.3.1). As σ is injective, σ induces an injection of E into E, so a bijection of E; the map $\lambda : G \to S_E$ defined by $\lambda(\sigma) = \sigma|E$ is an injective homomorphism of groups since E generates N. This gives the identification of G with a subgroup $\lambda(G)$ of S_E.

Let $x_1, \dots, x_n$ be the roots of P; then we can define a bijection $\varphi : \{1, \dots, n\} \to E$ with $x_i = \varphi(i)$. Such a bijection makes it possible to define an injective group homomorphism $\Phi : G \to S_n$ such that $s = \Phi(\sigma)$ is the permutation given by $\sigma(x_i) = x_{s(i)}$. This construction makes it possible to identify G with a subgroup $\Phi(G)$ of S_n.

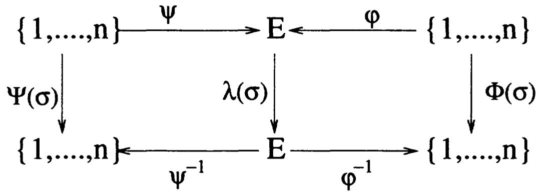


FIGURE 8.1.

Let $\varphi, \psi : \{1, \ldots, n\} \to E$ be two bijections. They define injective homomorphisms $\Phi, \Psi : G \to S_n$ by $\Phi(\sigma) = \varphi^{-1}\lambda(\sigma)\varphi$ and $\Psi(\sigma) = \psi^{-1}\lambda(\sigma)\psi$ (Figure 8.1). Thus, we associate to G the groups $\Phi(G)$ and $\Psi(G)$; these groups are mutually conjugate in S_n since $\psi^{-1}\varphi\Phi(G)\varphi^{-1}\psi = \Psi(G)$.

2) This is an immediate consequence of 1) and Lagrange's theorem.

3) For every i and every $j \in \{1, \ldots, n\}$, there exists a K-homomorphism from $K[x_i]$ to $K[x_j]$ by §6.3.1. This extends to an embedding of N in $\mathbb{C}$ which, as N is normal, induces an element σ of G such that $\sigma(x_i) = x_j$. ◇

8.1.5 A Short History of Groups

The first proof which actually uses the idea of a group is due to Lagrange (1770).

In attempting to determine the degree of the equation (whose coefficients were rational functions in the elementary symmetric polynomials) satisfied by a rational function $f = f(X_1, \ldots, X_n)$, he formed the product

$$\theta(t) = \prod_{\sigma \in S_n} \left(t - f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})\right)$$

and tried to write it in the form $\theta_1(t)^k$. For every σ in S_n, set $\sigma \cdot f = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$, and take the natural action of the group S_n on $E = \{\sigma \cdot f, \sigma \in S_n\}$; then the product of the cardinal of the orbit $O(f)$ by the cardinal k of the stabilizer $S(f)$ is $n!$, and we have $\theta(t) = \theta_1(t)^k$.

Obviously, this was not the language used by Lagrange; he reasoned on a special case. If $f(x', x'', x''', x^{IV}, \ldots) = f(x'', x''', x', x^{IV}, \ldots)$, then every other value of f is also taken twice, as he showed by the example

$$f(x^{IV}, x''', x', x'', \ldots) = f(x''', x', x^{IV}, x'', \ldots).$$

Then, he asserted, the same holds in the other cases. Who would dare to write this way nowadays? And yet, his argument is the basis of the argument used to prove that every equivalence class of elements in a group modulo a subgroup contains the same number of elements.

Galois was the first to actually use the word "group", but he meant it as a subgroup of the permutation group of the set of roots of a polynomial, as in Proposition 8.1.4. Galois did not use the notation for permutations

that we use now; he wrote successive arrangements of the roots which he called *permutations*:

abcde
bcdea
cdeab
...

emphasizing the fundamental notion of what he calls *substitution*, which makes it possible to pass from one *permutation* to another. Galois did not use associativity, identity elements, or inverses, only the internal group law, writing: "Thus, if in such a group we have the substitutions S and T, we are sure to have the substitution ST." Indeed, for a subset of S_n to be a subgroup, it is necessary and sufficient for it to be stable under composition.

The abstract form of the definition of a group, which we use today, was built up slowly over the course of the 19th century, with suggested definitions by Cayley (1854), Kronecker (1870), Weber (1882), Burnside (1897), and Pierpont (1900). The axioms of associativity, identity element and inverses were first stated in their present form by Pierpont.

8.2 Fields of Invariants

8.2.1 Definition and Proposition

Let K be a field, and let L be an extension of K and H a subgroup of $\mathrm{Gal}(L|K)$. *The set $I(H)$ of elements $x \in L$ invariant under H, i.e. such that for every $\sigma \in H$ we have $\sigma(x) = x$, is a subfield of L called the field of invariants of H (Figure 8.2).*

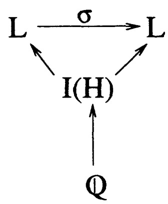


FIGURE 8.2.

8.2.2 Emil Artin's Theorem

Let K be a field, and let $L \subset \mathbb{C}$ be an extension of K and H a finite subgroup of order r of $\mathrm{Gal}(L|K)$. *Then L is a normal extension of $I(H)$ of degree r, and* $\mathrm{Gal}(L|I(H)) = H$.

PROOF. – Let $x \in L$, and let us show that x is of degree less than or equal to r over $I(H)$, and that its minimal polynomial P over $I(H)$ has all its roots in L.

The set $E = \{h(x), h \in H\}$ is finite, say of order t with $(t \leq r)$. For every i, $1 \leq i \leq t$, there exists h_i in H such that $\{h_i(x), 1 \leq i \leq t\} = E$. We set $S(X) = \prod_{1 \leq i \leq t} (X - h_i(x))$; it is a polynomial in $L[X]$. Let us show that the coefficients of S lie in $I(H)$.

Let $h \in H$. For every i with $1 \leq i \leq t$, we have $h(h_i(x)) \in E$; as h is injective and E is finite, we have $h(E) = E$.

Let $h' : L[X] \to L[X]$ be the algebra endomorphism defined by $h'|L = h$ and $h'(X) = X$, i.e. by $h'\left(\sum a_k X^k\right) = \sum h(a_k)X^k$. By the above, we have

$$\begin{aligned} h'(S)(X) &= \prod_{1 \leq i \leq t} h'(X - h_i(x)) \\ &= \prod_{1 \leq i \leq t} (X - h(h_i(x))) \\ &= \prod_{1 \leq i \leq t} (X - h_i(x)) \\ &= S(X). \end{aligned}$$

The coefficients of S are thus invariant under the elements of H and belong to $I(H)$.

Furthermore, E contains x since the identity map of L belongs to H, so $S(x) = 0$; thus x is algebraic over $I(H)$ and its minimal polynomial P divides S. It follows that x is of degree less than or equal to $t = \deg(S)$, so less than or equal to r over $I(H)$. As S factors into linear factors in L, the same holds for P: all the roots of P lie in L. Thus L is a normal extension of $I(H)$.

Let us now show that L is an extension of finite degree r of $I(H)$. As every element $x \in L$ is of degree $\leq r$ over $I(H)$, we can set s to be the maximum of the degrees of the elements of L over $I(H)$. Let y be an element of degree s. If $I(H)[y]$ is strictly contained in L, then there exists z in $L - I(H)[y]$; z is algebraic over $I(H)$, so it is algebraic over $I(H)[y]$ and $[I(H)[y][z] : I(H)] > [I(H)[y] : I(H)] = s$. By the Primitive Element Theorem (§6.5), there exists an element w of L such that $I(H)[y][z] = I(H)[w]$ (Figure 8.3).

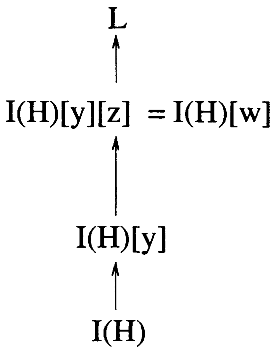


FIGURE 8.3.

We thus have $[I(H)[w] : I(H)] > s$, which contradicts the maximality of s. Hence $L = I(H)[y]$, so L is an extension of finite degree of $I(H)$ and $[L : I(H)] = s \leq r$. Finally, $\left|\text{Gal}(L|I(H)\right| = [L : I(H)]$, by §8.1.2; as $H \subset \text{Gal}(L|I(H)$, we have $r \leq [L : I(H)]$ so that $r = [L : I(H)]$ and $H = \text{Gal}(L|I(H)$. ◇

8.3 The Example of $\mathbf{Q}\left[\sqrt[3]{2}, j\right]$: First Part

We know that the splitting field of $X^3 - 2$ over $\mathbb{Q}$ is the normal extension $N = \mathbb{Q}\left[\sqrt[3]{2}, j\right]$. As $[N : \mathbb{Q}] = 6$, the Galois group $G = \text{Gal}(N|\mathbb{Q})$ has six elements; let us call them $\sigma_1, \ldots, \sigma_6$. For $1 \leq i \leq 6$, σ_i is determined by the images of j and $\sqrt[3]{2}$, which are conjugates of these elements over $\mathbb{Q}$. The image of j is j or j^2; the image of $\sqrt[3]{2}$ is $\sqrt[3]{2}$, $j\sqrt[3]{2}$, or $j^2\sqrt[3]{2}$. This gives the six possibilities listed in Table 8.1.

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\sqrt[3]{2}$	$j\sqrt[3]{2}$	$j\sqrt[3]{2}$	$j^2\sqrt[3]{2}$	$j^2\sqrt[3]{2}$
j	j	j^2	j	j^2	j	j^2

TABLE 8.1.

Note that σ_1 is the identity on N and the identity element of G, and that σ_2 is induced by complex conjugation.

To determine the structure of G, we note that it has three elements of order two: $\sigma_2, \sigma_4, \sigma_6$, and two elements of order 3: σ_3, σ_5. Thus it is isomorphic to S_3 (the only other group with six elements is the cyclic group $(\mathbb{Z}/6\mathbb{Z}, +)$, which contains only one element of order two). We can also note that G is a group with six elements, and since it can be identified with a subgroup of S_3, by §8.1.4, it must be isomorphic to S_3.

If we number the three roots of $X^3 - 2$, for example if we number $\sqrt[3]{2}$ as 1, $j\sqrt[3]{2}$ as 2 and $j^2\sqrt[3]{2}$ as 3, we construct an isomorphism from G to S_3 (Table 8.2).

σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
id	(23)	(123)	(12)	(132)	(13)

TABLE 8.2.

Let us determine the field of invariants of a subgroup H of G.

If $H = \{\text{id}\}$, it is clear that $I(H) = N$.

Recall that every element x of N can be written uniquely in the form

$$x = a + bj + c\sqrt[3]{2} + dj\sqrt[3]{2} + e\sqrt[3]{4} + fj\sqrt[3]{4}.$$

If $H = \langle\sigma_3\rangle$, then x belongs to $I(H)$ if $x = \sigma_3(x)$; i.e.

$$x = a + bj + cj\sqrt[3]{2} + d(-1-j)\sqrt[3]{2} + e(-1-j)\sqrt[3]{4} + f\sqrt[3]{4},$$

which implies that $c = -d$, $d = c - d$, $e = -e + f$, $f = -e$, i.e. $c = d = e = f = 0$.

Thus $I(H) = \mathbb{Q}[j]$. As shown by Artin's theorem, we indeed have $[N : \mathbb{Q}[j]] = 3 = |H|$ and $\mathrm{Gal}(N|\mathbb{Q}[j]) = H$.

Similarly, we find

$$I(\langle\sigma_2\rangle) = \mathbb{Q}\left[\sqrt[3]{2}\right], \qquad I(\langle\sigma_4\rangle) = \mathbb{Q}\left[j^2\sqrt[3]{2}\right], \qquad I(\langle\sigma_6\rangle) = \mathbb{Q}\left[j\sqrt[3]{2}\right].$$

If $H = G$, all of the preceding conditions must be satisfied, so we find that $I(H) = \mathbb{Q}$.

The correspondence between the set of subgroups of S_3 (or of G), ordered by inclusion, and the set of the intermediate extensions between $\mathbb{Q}$ and N, also ordered by inclusion, is just one example of the central tenet of Galois theory, the *Galois correspondence*, which we will study in §8.5. It is summarized in Figure 8.4.

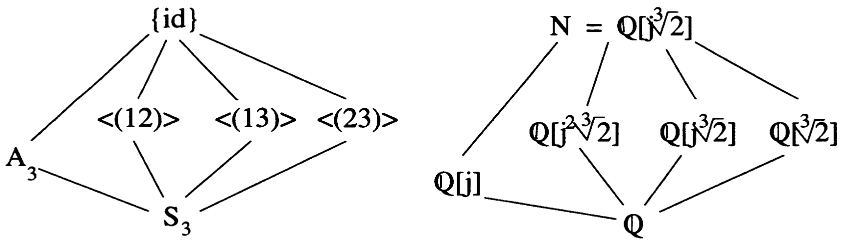


FIGURE 8.4.

8.4 Galois Groups and Intermediate Extensions

PROPOSITION. – *Let K be a field. Let N be a normal extension of finite degree of K and L an intermediate extension between K and N. We know (see §7.5) that N is a normal extension of L. We also assume that L is a normal extension of K (Figure 8.5).*

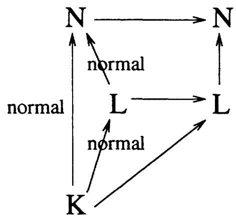


FIGURE 8.5.

1) The map $\varphi : \mathrm{Gal}(N|K) \to \mathrm{Gal}(L|K)$ obtained by taking the restriction to L of a K-automorphism of N is a surjective group homomorphism with kernel equal to $\mathrm{Gal}(N|L)$.

2) The group $\mathrm{Gal}(N|L)$ *is a normal subgroup of* $\mathrm{Gal}(N|K)$, *and*

$$\mathrm{Gal}(N|K)/\mathrm{Gal}(N|L) \simeq \mathrm{Gal}(L|K).$$

COMMENTARY. – We thus have the following exact sequence of (not necessarily abelian) groups:

$$1 \to \mathrm{Gal}(N|L) \to \mathrm{Gal}(N|K) \xrightarrow{\varphi} \mathrm{Gal}(L|K) \to 1.$$

In other words, $\mathrm{Gal}(N|K)$ is a (group) extension of $\mathrm{Gal}(N|L)$ by $\mathrm{Gal}(L|K)$.

PROOF. – 1) φ is a group homomorphism. By §6.4.3, it is surjective. Moreover, if $\sigma \in \ker(\varphi)$, then $\sigma|L = \mathrm{id}(L)$, so $\sigma \in \mathrm{Gal}(N|L)$ and $\ker(\varphi) \subset \mathrm{Gal}(N|L)$. The converse is obvious.

2) We know that the kernel of a group homomorphism is a normal subgroup; the isomorphism is a consequence of a classical theorem on quotients. ◊

8.5 The Galois Correspondence

As promised at the beginning of this chapter, we now come to the very heart of Galois theory.

FUNDAMENTAL THEOREM OF GALOIS THEORY. – *Let K be a field, and let N be a normal extension of finite degree of K. Let $\mathcal{E}$ be the set of*

intermediate extensions between K *and* N*, and let* $\mathcal{G}$ *be the set of subgroups of* $\text{Gal}(N|K)$*.*

Let $I : \mathcal{G} \to \mathcal{E}$ *denote the map which associates to a subgroup* H *of* $\text{Gal}(N|K)$ *the field of invariants* $I(H)$*, and let* $G : \mathcal{E} \to \mathcal{G}$ *be the map which associates to an extension* L *of* $\mathcal{E}$ *the group* $\text{Gal}(N|L)$*.*

1) I *and* G *define inverse bijections which are decreasing for the inclusion relation.*

2) By restriction, I *and* G *define inverse bijections of the set* $\mathcal{E}'$ *of normal extensions of* K *contained in* N *to the set* $\mathcal{G}'$ *of normal subgroups of* $\text{Gal}(N|K)$*.*

3) If L *and* L' *are intermediate extensions between* K *and* N*, then* L' *is a normal extension of* L *if and only if* $\text{Gal}(N|L')$ *is a normal subgroup of* $\text{Gal}(N|L)$*, in which case* $\text{Gal}(L'|L) = \text{Gal}(N|L)/\text{Gal}(N|L')$*.*

4) If L *and* L' *are intermediate extensions between* K *and* N *with* $L' \supset L$*, then*

$$[L' : L] = |\text{Gal}(N|L)| \,/\, |\text{Gal}(N|L')|.$$

COMMENTS. –

1) I and G define a *trellis isomorphism.* Let us explain this.

Recall that the expression $z = \sup(x, y)$ in an ordered set means that z is the smallest element satisfying $z \geq x$ and $z \geq y$, i.e. for every t such that $t \geq x$, $t \geq y$, we have $t \geq z$. The definition of $z = \inf(x, y)$ is analogous. A *trellis* is an ordered set in which the sup and the inf of any two elements exists.

$\mathcal{E}$ is a trellis for inclusion, since $\inf(L, L') = L \cap L'$ and $\sup(L, L') = K(L \cup L')$.

$\mathcal{G}$ is a trellis for inclusion: indeed, if H and H' are subgroups of $\text{Gal}(N|K)$, then $\inf(H, H') = H \cap H'$ and $\sup(H, H')$ is the subgroup generated by H and H'.

2) This theorem asserts in particular that an element of N lies in K if it is invariant under all of the elements of $\text{Gal}(N|K)$, a result that is often useful.

PROOF. – 1) The fact that I and G are decreasing is clear.

Let us show that $I \circ G = \text{id}(\mathcal{E})$. Let $L \in \mathcal{E}$ and $L' = I(G(L))$. N is a normal extension of L and L'. We have $L' \supset L$ since every $\sigma \in G(L) = \text{Gal}(N|L)$ satisfies $\sigma|L = \text{id}(L)$. As G is decreasing, we have $G(L') \subset G(L)$; moreover, if $\sigma \in G(L)$, we have $\sigma|L' = \text{id}(L')$ by definition of L'. Thus, $\sigma \in G(L')$, so that $G(L) = G(L')$. As $|G(L)| = [N : L]$ and $|G(L')| = [N : L']$, we have $[L' : L] = 1$, so $L' = L$.

The equality $G \circ I = \mathrm{id}(\mathcal{G})$ was the object of Artin's theorem (Theorem 8.2.2).

2) Proposition 8.4 shows that if L lies in $\mathcal{E}'$, then $G(L)$ is a normal subgroup of $\mathrm{Gal}(N|K)$. Conversely, if H lies in $\mathcal{G}'$, let us show that $I(H)$ lies in $\mathcal{E}'$ by using §7.3. Let $\sigma : I(H) \to L \subset N$ be a K-homomorphism. As N is a normal extension of finite degree of $I(H)$, there exists a K-automorphism τ of N such that $\tau|I(H) = \sigma$. For every ρ of $\mathrm{Gal}(N|I(H)) = G(I(H)) = H$, we have $\tau^{-1}\rho\tau \in H$ since H lies in $\mathcal{G}'$. Consequently, for every x in $I(H)$, we have $\tau^{-1}\rho\tau(x) = x$, so that $\tau(x) = \rho(\tau(x))$, which shows that $\sigma(x) = \tau(x) \in I(H)$ by 1); $I(H)$ is indeed a normal extension of K.

3) It suffices to apply 2), replacing K By L, and Proposition 8.4.

4) Indeed, we have

$$|\mathrm{Gal}(N|L)| \,/\, |\mathrm{Gal}(N|L')| = [N|L]/[N|L'] = [L' : L]. \qquad \diamond$$

8.6 The Example of $\mathbf{Q}\left[\sqrt[3]{2}, j\right]$: Second Part

In this example, $A_3 = \langle(123)\rangle$ is the only non-trivial normal subgroup of S_3, and the normal extension $\mathbb{Q}[j]$ of $\mathbb{Q}$ corresponds to it.

Let us give the computation of Proposition 8.4 in detail. $\mathrm{Gal}(N|\mathbb{Q})$ has six elements which we denoted by $\sigma_1, \ldots, \sigma_6$. $\mathrm{Gal}(N|\mathbb{Q}[j])$ is the subgroup consisting of the elements $\sigma_1, \sigma_3, \sigma_5$. We have

$$\mathrm{Gal}(\mathbb{Q}[j]|\mathbb{Q}) \simeq \mathrm{Gal}(N|\mathbb{Q})/\mathrm{Gal}(N|\mathbb{Q}[j]) \simeq \mathbb{Z}/2\mathbb{Z};$$

the elements of $\mathrm{Gal}(\mathbb{Q}[j]|\mathbb{Q})$ are the restrictions of the elements of $\mathrm{Gal}(N|\mathbb{Q})$ to $\mathbb{Q}[j]$. Restricted to $\mathbb{Q}[j]$, $\sigma_1, \sigma_3, \sigma_5$ act like the identity and $\sigma_2, \sigma_4, \sigma_6$ act like complex conjugation.

8.7 The Example $X^4 + 2$

In the following chapters, we will see classes of polynomials for which one can actually compute the Galois group. We refer to Chapter 16 for a sketch of algorithmic methods used for polynomials of small degree; in this section, we give one rather long, complete example. We need to begin by recalling dihedral groups.

8.7.1 Dihedral Groups

The group dihedral D_n is the group of isometries of a regular polygon with $n \geq 3$ sides. As an isometry preserves barycenters, it preserves the center O of the polygon, the isobarycenter of the set of vertices, and induces a permutation of the vertices of the polygon.

Let $A_0, A_1, \ldots, A_{n-1}$ be the n vertices of the polygon. An isometry f is determined by the images of A_0 and A_1. If $f(A_0) = A_k$, $f(A_1)$ is A_{k-1} or

A_{k+1} (we consider the indices modulo n) since f conserve the distances. If $f(A_1) = A_{k+1}$, then f is the rotation of center O and angle $2k\pi/n$. If $f(A_1) = A_{k-1}$, f is the symmetry with respect to line D passing through O such that $(OA_0, D) = k\pi/n$.

Let r denote the rotation of angle $2\pi/n$ and s the symmetry with respect to OA_0. Thus, the dihedral group D_n has $2n$ elements:

1) the rotations of angles $2k\pi/n$, equal to r^k for $0 \leq k \leq n-1$; and

2) the symmetries with respect to the lines D passing through O such that $(OA_0, D) = k\pi/n$, with $0 \leq k \leq n-1$; they are equal to $r^k s$ since $r^k s(A_0) = A_k$ and $r^k s(A_1) = A_{k-1}$.

The group D_n is thus generated by r and s, and in order to perform all computations in the group D_n, it suffices to use the three relations: $r^n = \text{id}$, $s^2 = \text{id}$, $sr = r^{-1}s$. The two first relations are obvious, and the third is a consequence of the fact that $sr(A_0) = A_{n-1} = r^{-1}s(A_0)$ and $sr(A_1) = A_{n-2} = r^{-1}s(A_1)$. It follows that $sr^k = r^{-k}s$. We prove that if a group is generated by two elements satisfying these three properties, it is a quotient of D_n, and these relations characterize D_n among all groups of order $2n$.

8.7.2 The Special Case of D_4

We will see in §8.7.3 below that the structure of the Galois group of the polynomial $X^4 + 2$ over $\mathbb{Q}$ is that of the group D_4. Let us recall some properties of this group, its subgroups, and its embeddings in S_4, so as to highlight the Galois correspondence.

The group D_4 is the group of isometries of a square $ABCD$. Let Δ and Δ' denote the mediatrices of (AB) and (BC) (Figure 8.6).

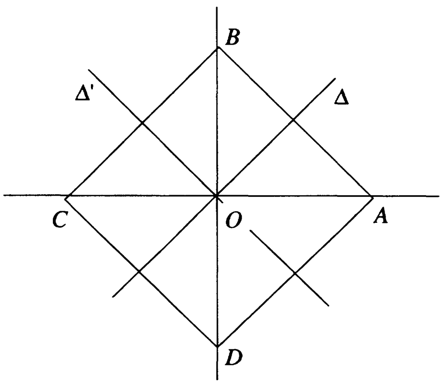


FIGURE 8.6.

The group D_4 contains eight elements: the identity, two elements of order 4, $r = \text{rot}(O, \pi/2)$ and $r^3 = \text{rot}(O, -\pi/2) = r^{-1}$, and five elements of order 2, $r^2 = \text{rot}(O, \pi) = -id = \text{sym}/O$, $s = \text{sym}/(CA)$, $rs = \text{sym}/\Delta = sr^3$, $r^2 s = \text{sym}/(BD) = sr^2$, and $r^3 s = \text{sym}/\Delta' = sr$.

The subgroups of D_4 have 1, 2, 4, or 8 elements. The subgroup with one element is $\{\text{id}\}$; the subgroups with two elements are $\langle r^2 \rangle = \{\text{id}, \text{r}^2\}$, $\langle s \rangle$, $\langle rs \rangle$, $\langle r^2 s \rangle$, $\langle r^3 s \rangle$; the subgroups with four elements are $\langle r \rangle$, $\langle s, r^2 s \rangle = \{\text{id}, \text{s}, \text{r}^2\text{s}, \text{r}^2\}$, $\langle rs, r^3 s \rangle = \{\text{id}, \text{rs}, \text{r}^3\text{s}, \text{r}^2\}$; the subgroup with eight elements is D_4 itself. The notation $\langle x_1, \ldots, x_n \rangle$ means the subgroup generated by the elements $x_1, \ldots, x_n$. One of the subgroups with four elements is cyclic of order 4, and the other two are generated by symmetries defined by two orthogonal lines: (AC) and (BD) or Δ and Δ'; showing that these are the only subgroups is a simple matter of patience.

Every bijection $\{A, B, C, D\} \to \{1, 2, 3, 4\}$ defines an embedding of D_4 into S_4, but there are only three distinct subgroups of S_4 isomorphic to D_4 (a quick proof is given by the Sylow theorems; see Exercise 8.2).

8.7.3 The Galois Group of $X^4 + 2$

The polynomial $X^4 + 2$ is irreducible over $\mathbb{Q}$. Its roots in $\mathbb{C}$ are $\pm\zeta\sqrt[4]{2}$ and $\pm i\zeta\sqrt[4]{2}$, where $\zeta = e^{i\pi/4} = (1+i)/\sqrt{2}$. The splitting field of $X^4 + 2$ is thus $N = \mathbb{Q}[\zeta\sqrt[4]{2}, i\zeta\sqrt[4]{2}]$. As $N \subset \mathbb{Q}[\sqrt[4]{2}, i]$ and $\zeta\sqrt[4]{2} - i\zeta\sqrt[4]{2} = 2 \times 2^{-1/4}$, $\sqrt[4]{2}$ lies in N, so $N = \mathbb{Q}[\sqrt[4]{2}, i]$.

We see that $[N : \mathbb{Q}] = 8$ since $\sqrt[4]{2}$ is of degree 4 over $\mathbb{Q}$ and i is of degree 2 over $\mathbb{Q}[\sqrt[4]{2}]$. Thus, the Galois group G of $X^4 + 2$ is of order 8. We also know that it is a subgroup of S_4. Using the Sylow theorems, we can assert that $G \simeq D_4$ without even giving an explicit isomorphism.

This is not sufficient for our purposes, because we want to use the group D_4 as a *model group*, in the sense that we know how to determine its subgroups, normal subgroups, etc., and can transport this information into G by explicit isomorphism.

To define the elements of G, it suffices to give their value at $\sqrt[4]{2}$ and i, as we saw in Chapter 6. Defining ρ and σ by $\rho(\sqrt[4]{2}) = i\sqrt[4]{2}$, $\rho(i) = i$ and $\sigma(\sqrt[4]{2}) = \sqrt[4]{2}$, $\sigma(i) = -i$, we can check that ρ is of order 4 and σ of order 2, and that ρ and σ generate G and the eight elements of G are defined as in Table 8.3.

In this table, we added columns giving the images of the remarkable elements $\sqrt{2}$ and ζ, although these can of course be deduced from the other columns. An isomorphism $\varphi : D_4 \to G$ is strongly suggested by the notation, namely the one defined by $\varphi(r) = \rho$, $\varphi(s) = \sigma$, etc.

8.7.4 The Galois Correspondence

Using the isomorphism $\varphi : D_4 \to G$ defined in §7.3, we obtain the subgroups of G as the images of those of D_4. They are given by $\{\text{id}\}$, $\langle \rho^2 \rangle$, $\langle \sigma \rangle$, $\langle \rho\sigma \rangle$,

	$\sqrt[4]{2}$	i	$\sqrt{2}$	ζ
id	$\sqrt[4]{2}$	i	$\sqrt{2}$	ζ
ρ	$i\sqrt[4]{2}$	i	$-\sqrt{2}$	$-\zeta$
ρ^2	$-\sqrt[4]{2}$	i	$\sqrt{2}$	ζ
ρ^3	$-i\sqrt[4]{2}$	i	$-\sqrt{2}$	$-\zeta$
σ	$\sqrt[4]{2}$	$-i$	$\sqrt{2}$	$-i\zeta$
$\rho\sigma$	$i\sqrt[4]{2}$	$-i$	$-\sqrt{2}$	$i\zeta$
$\rho^2\ \sigma$	$-\sqrt[4]{2}$	$-i$	$\sqrt{2}$	$-i\zeta$
$\rho^3\ \sigma$	$-i\sqrt[4]{2}$	$-i$	$-\sqrt{2}$	$i\zeta$

TABLE 8.3.

$\langle\rho^2\sigma\rangle$, $\langle\rho^3\sigma\rangle$, $\langle\sigma, \rho^2\sigma\rangle$, $\langle\rho\sigma, \rho^3\sigma\rangle$, $\langle\rho\rangle$, and G itself. We can then proceed to completely determine the trellis of intermediate extensions between $\mathbb{Q}$ and N, and its Galois correspondence with the trellis of subgroups of G (Figure 8.7).

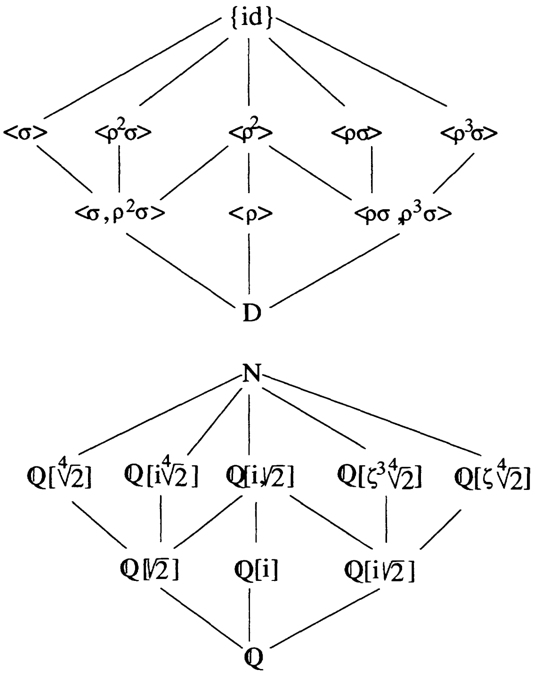


FIGURE 8.7. Trellis of subgroups and the corresponding intermediate extensions

Do not forget that some intermediate extensions are obvious once we know that $N = \mathbb{Q}[\sqrt[4]{2}, i] : \mathbb{Q}[\sqrt[4]{2}], \mathbb{Q}[i], \mathbb{Q}[\sqrt{2}]$, etc. Using the table of values of ρ and σ and the degrees of these extensions, we see to which subgroups they correspond. For example, $\mathbb{Q}[i\sqrt{2}]$ is of degree 2 over $\mathbb{Q}$, so it corresponds to a subgroup with $8/2 = 4$ elements. As $\rho\sigma(i\sqrt{2}) = i\sqrt{2}$ and $\rho^2(i\sqrt{2}) = i\sqrt{2}$, this subgroup is necessarily given by $\langle \rho\sigma, \rho^3\sigma \rangle$. Thus, $\mathbb{Q}[i\sqrt{2}] = I(\langle \rho\sigma, \rho^3\sigma \rangle)$.

To identify $I(\langle \rho\sigma \rangle)$, in the absence of a better idea, we need to have recourse to linear algebra. A basis of N over $\mathbb{Q}$ is given by 1, $\sqrt[4]{2}$, $\sqrt{2}$, $\sqrt[4]{8}$, i, $i\sqrt[4]{2}$, $i\sqrt{2}$, and $i\sqrt[4]{8}$. For

$$x = a + b\sqrt[4]{2} + c\sqrt{2} + d\sqrt[4]{8} + ei + fi\sqrt[4]{2} + gi\sqrt{2} + hi\sqrt[4]{8},$$

with coefficients in $\mathbb{Q}$, the equality $x = \rho\sigma(x)$ implies that $b = f$, $c = e = 0$, $h = -d$; we are tempted to set $\alpha = (1+i)\sqrt[4]{2}$ and note that $x = a + b\alpha + g'\alpha^2 + d'\alpha^3$ with coefficients in $\mathbb{Q}$, giving $I(\langle \rho\sigma \rangle) = \mathbb{Q}[\alpha]$. Note that $\mathbb{Q}[\alpha] = \mathbb{Q}[\zeta^3\sqrt[4]{2}]$. Similarly, we find that $I(\langle \rho^3\sigma \rangle) = \mathbb{Q}[\zeta\sqrt[4]{2}]$.

Looking for normal extensions in the trellis of extensions between $\mathbb{Q}$ and N is equivalent to looking for normal subgroups in the trellis of subgroups between $\{\mathrm{id}\}$ and G. The trivial normal subgroups G and $\{\mathrm{id}\}$ correspond to $\mathbb{Q}$ and N. The subgroups of index 2 are all normal, and the corresponding extensions of degree 2 are obviously normal. The only non-trivial case is that of the subgroup $\langle \rho^2 \rangle$, corresponding to the normal subgroup $\langle r^2 \rangle$ of D_4; it corresponds to the normal extension $\mathbb{Q}[i, \sqrt{2}]$ of $\mathbb{Q}$. Even if we already knew, before reading this chapter, that these extensions of $\mathbb{Q}$ are normal, we can now assert that they are the only normal ones in the trellis of extensions between $\mathbb{Q}$ and N.

8.7.5 Search for Minimal Polynomials

Knowing the Galois group gives a new way of finding the minimal polynomial of an element of a normal extension.

For example, to find the minimal polynomial P of $\alpha = i + \zeta$ over $\mathbb{Q}$, we look for the set of conjugates of α over $\mathbb{Q}$; this is the set of images of α under the elements of G, and we note that this set contains exactly four elements: α, $i - \zeta = \rho(\alpha)$, $-i - i\zeta = \sigma(\alpha)$, $-i + i\zeta = \rho\sigma(\alpha)$. After some longish computations, we obtain

$$\begin{aligned} P(X) &= (X - i - \zeta)(X - i + \zeta)(X + i + i\zeta)(X + i - i\zeta) \\ &= X^4 + 2X^2 + 4X + 2. \end{aligned}$$

Toward Chapters 9, 10, and 12

It is now possible to give some important applications of Galois theory: to roots of unity, first of all, then to extensions with cyclic Galois group, and finally to the problem of solvability by radicals.

Exercises for Chapter 8

In the two first exercises, we collect the basic facts about group actions on sets, and the Sylow theorems necessary to understand some parts of the main text. The solutions are contained in all classic algebra books.

Exercise 8.1. Groups acting on sets

We say that a group G *acts on a set* E if there exists a group homomorphism $\varphi : G \to S_E$ where S_E is the permutation group of E, i.e. the set of bijections of E to itself. For every $g \in G$ and every $x \in E$, the action of g on x gives an element which we denote by $g \cdot x = \varphi(g)(x)$. In this exercise, we show the following properties:

1) $e \cdot x = x$ for every $x \in E$, where e is the identity element of G;

2) $(gh) \cdot x = g \cdot (h \cdot x)$ for every $x \in E$ and every $g, h \in G$.

Some frequently encountered examples are the action of a subgroup of S_n acting on the set $\{1, \dots, n\}$, the actions of geometric groups on a set of points in the plane (rotations of the points on a circle, etc.), the action of a group on itself or on one of its quotients by left translation, the action of a group acting on the set of its subgroups by conjugation, and the action of the Galois group of a polynomial acting on its roots.

We define the orbit of a point $x \in E$ under the action of G by $O_G(x) = \{g \cdot x, g \in G\}$, and the stabilizer $S_G(x)$ by $S_G(x) = \{g \in G, g \cdot x = x\}$. We simply write $O(x)$ and $S(x)$ when there is no danger of confusion.

We say that G acts transitively if the whole set forms a single orbit, i.e. if for every $x, y \in E$, there exists g in G such that $y = g \cdot x$. A transitive subgroup of S_n is a subgroup of S_n which acts transitively on $\{1, \dots, n\}$.

In what follows, we assume that G and E are finite.

1) Show that $S(x)$ is a subgroup of G and that $|S(x)||O(x)| = |G|$.

2) **a)** Let x and y be two elements belonging to the same orbit, so that $y = \gamma \cdot x$ for some $\gamma \in G$. Show that $S(x)$ and $S(y)$ are conjugate subgroups; more precisely, show that $S(y) = \gamma S(x) \gamma^{-1}$.

b) If G acts transitively on E, show that the stabilizers of the elements of E all have the same number of elements.

3) Let p be a prime. We say that a group is a *p-group* if its order is a power of p.

a) Burnside's theorem: Show that a non-trivial p-group has a non-trivial normal subgroup, namely its center, by letting G act on the set of its conjugacy classes (the *conjugacy class* of an element $x \in G$ is the set $\{gxg^{-1}, g \in G\}$), and counting the elements modulo p.

b) Show that a group of order p^2 is necessarily commutative.

Exercise 8.2. The Sylow theorems

The Norwegian mathematician Ludwig Sylow (1832-1918) was extremely interested in the work of Abel and Galois; he even wrote their biographies. His results on finite groups, published in 1872, are extremely useful.

If a prime number p divides the order of a finite group G, we define a *p-subgroup* of G to be any subgroup of G whose order is a power of p, and a *Sylow p-subgroup* of G to be any p-subgroup of G whose order is the maximal power of p dividing $|G|$. Let m_p denote the number of Sylow p-subgroups. The Sylow theorems assert that

1) every p-subgroup of G is contained in a Sylow p-subgroup of G;

2) $m_p = 1 \bmod p$ (so $m_p \neq 0$; one easy consequence of this result is Cauchy's theorem proving the existence of elements of order p in G);

3) the group G acts transitively by conjugation on the set of its Sylow p-subgroups, which implies that any two Sylow p-subgroups of G are conjugate, so that in particular m_p divides $|G|$ and that if $m_p = 1$, the unique Sylow p-subgroup of G is normal in G.

The Sylow theorems are particularly interesting for groups whose order is not a prime power. Using the relations $m_p = 1 \bmod p$ and the fact that m_p divides $|G|$, we can list the possible values of m_p for a given group G; if $|G|$ is small, there are not many possibilities.

Exercise 8.3. Non-normal extensions

Set $L = \mathbb{Q}[\sqrt[3]{2}, \sqrt[5]{3}]$. Determine $G = \mathrm{Gal}(L|\mathbb{Q})$. Does the Galois correspondence hold here?

Exercise 8.4. Computation of Galois groups

For each of the following polynomials P of degree n, determine:

- the Galois group G of the splitting field N of P over $\mathbb{Q}$;
- the correspondence between subgroups of G and subextensions of N;
- the factorization of P over each of its intermediate extensions;
- a subgroup of S_n isomorphic to G, by numbering the roots.

1) $X^2 - 2$; **2)** $(X^2 - 2)(X^2 - 3)$;
3) $X^3 - 1$; **4)** $X^3 + 2$;
5) $X^4 + 1$; **6)** $X^4 - 1$.

Exercise 8.5. Galois groups

1) Let N be a normal extension of finite degree of a field K. Let H be a subgroup of $\mathrm{Gal}(N|K)$, and let $I(H)$ be the field of invariants under H. Show that $[I(H) : K] = |\mathrm{Gal}(N|K)/H|$.

2) Let $L \subset \mathbb{C}$ be an extension of finite degree of a field K, and let G be the Galois group of L over K. Show that if $|G| = [L : K]$, then L is a normal extension of K.

3) For every even integer $n \geq 2$, find a polynomial of degree n with distinct non-rational roots, whose Galois group over $\mathbb{Q}$ is $\mathbb{Z}/2\mathbb{Z}$.

4) Let $\mathbb{C}(X)$ be the field of rational functions in one indeterminate, and let G be the group of $\mathbb{C}$-automorphisms of $\mathbb{C}(X)$ consisting of the set of maps σ_a defined for every $a \in \mathbb{C}$ by

$$\sigma_a\left(\frac{P(X)}{Q(X)}\right) = \frac{P(X+a)}{Q(X+a)}.$$

Show that $I(G) = \mathbb{C}$.

Exercise 8.6. Galois groups that are direct products

1) Let K be a field, and let N be a normal extension of K. Let L' and L'' be extensions of K contained in N, and set $G = \mathrm{Gal}(N|K)$, $G' = \mathrm{Gal}(N|L')$ and $G'' = \mathrm{Gal}(N|L'')$. Show that if L' and L'' are normal extensions of K such that $L' \cup L''$ generates N and $L' \cap L'' = K$, then G is the direct product of its subgroups G' and G'', i.e. $G \simeq G' \times G''$.

2) Show the converse: if K is a field and N a normal extension of K, if $G = \mathrm{Gal}(N|K)$ is a direct product $G \simeq G' \times G''$, and if $L' = I(G')$

and $L'' = I(G'')$, then $L' \cup L''$ generates N and $L' \cap L'' = K$. (Recall that G is a *direct product* of two of its subgroups H and K if

a) H and K are normal subgroups of G;

b) $H \cap K = \{e\}$;

c) $HK = \{hk, h \in H, k \in K\} = G$.)

3) Show that, under the conditions of **1)**, we have

$$\mathrm{Gal}(N|K) \simeq \mathrm{Gal}(L'|K) \times \mathrm{Gal}(L''|K).$$

Exercise 8.7. Cubic equations

Consider the polynomial $P(X) = X^3 + pX + q$. Write a, b, c for its roots and D for its discriminant, and let d be a complex number such that $d^2 = D$, $K = \mathbb{Q}(p, q)$, $G = \mathrm{Gal}(K[a, b, c]|K)$.

1) Assume that P is reducible over K. What are the possible structures of G? Give them in terms of d.

2) Assume that P is irreducible over K. What are the possible group structures on G? (Distinguish between the case $d \in K$ and the case $d \notin K$.) Give the intermediate extensions between K and $K[a, b, c]$ in each case.

3) Determine the Galois groups of

a) $X^3 - 2X - 1$ over $\mathbb{Q}$ and over $\mathbb{Q}[\sqrt{5}]$;

b) $X^3 - 3X + 1$ over $\mathbb{Q}$;

c) $X^3 - 4X + 1$ over $\mathbb{Q}$;

d) $X^3 - 2X + 2$ over $\mathbb{Q}$ and over $\mathbb{Q}[i\sqrt{19}]$;

e) $X^3 - 5$ over $\mathbb{Q}$, over $\mathbb{Q}[\sqrt[3]{5}]$ and over $\mathbb{Q}[i\sqrt{3}]$;

f) $X^5 + X^2 - 9X + 3$ over $\mathbb{Q}$.

Exercise 8.8. Biquadratic extensions

The fields we consider here are all intermediate extensions between $\mathbb{Q}$ and $\mathbb{C}$.

A *biquadratic extension* of a field K is an algebraic extension L of degree 4 of K such that there exist a and $b \in K$ with $L = K[\sqrt{a}, \sqrt{b}]$.

1) a) Show that every biquadratic extension N of a field K is normal; give its Galois group G and the Galois correspondence between subgroups of G and intermediate extensions between K and N.

b) Let N be a normal extension of degree 4 of a field K such that $\mathrm{Gal}(N|K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Show that N is a biquadratic extension of K.

2) Set $\alpha = \sqrt{6+\sqrt{11}}$, $\beta = \sqrt{6-\sqrt{11}}$, and $N = \mathbb{Q}[\alpha]$.

a) Determine the minimal polynomial P of α over $\mathbb{Q}$.

b) Compare $\mathbb{Q}[\sqrt{11}]$ and N. Show that β lies in N, and give its expression in the basis $\{1, \alpha, \alpha^2, \alpha^3\}$.

c) Show that N is a normal extension of degree 4 of $\mathbb{Q}$.

d) Set $G = \mathrm{Gal}(N|\mathbb{Q})$. What is the structure of G?

e) What are the degrees of $\alpha+\beta$ and $\alpha-\beta$ over $\mathbb{Q}$? Deduce that α and β can be written in the form $\sqrt{a} \pm \sqrt{b}$ for elements a and $b \in \mathbb{Q}$; compute a and b.

f) Give the trellis of intermediate extensions between $\mathbb{Q}$ and N.

Exercise 8.9. The normal closure of $\mathbb{Q}\left[\sqrt[3]{1+\sqrt{2}}\right]$

Set $P(X) = X^3 + 3X - 2$, $u = \sqrt[3]{1+\sqrt{2}}$ and $v = \sqrt[3]{1-\sqrt{2}}$, where the cube roots lie in $\mathbb{R}$. Let D be the discriminant of P, and let d be the number, with positive imaginary part, such that $d^2 = D$ and N is the normal closure of $\mathbb{Q}(u)$ over $\mathbb{Q}$.

1) Determine the number of real roots of P.

Now, let c, a, and b denote the roots of P with negative, zero, or positive imaginary parts respectively, and let Γ be the Galois group $\mathrm{Gal}(\mathbb{Q}[a,b,c]|\mathbb{Q})$.

2) Determine a, b, c and the structure of Γ.

3) What is the degree of u over $\mathbb{Q}$?

4) Show that $N = \mathbb{Q}[u, j]$.

5) Give examples of distinct non-trivial intermediate extensions between $\mathbb{Q}$ and N.

Now, let G be the Galois group $\mathrm{Gal}(N|\mathbb{Q})$.

6) Determine the order of G.

For what follows, one can proceed by constructing a table giving the values $g(x)$ for g in G and certain x in N.

7) Let $\sigma, \rho : N \to N$ denote the elements of G such that $\sigma(u) = u$, $\sigma(j) = j^2$, $\rho(u) = jv$, and $\rho(j) = j^2$. What are the orders of σ and ρ? Show that ρ and σ generate G. Compute $\rho(\sqrt{2}), \sigma(d)$, and $\rho(d)$.

8) What is the structure of G?

9) Which subgroup of G leaves $\mathbb{Q}[u]$ invariant? Is it a normal subgroup of G?

10) Determine the extensions invariant under the groups $\langle \sigma, \rho^2 \rangle$, $\langle \rho\sigma, \rho^2 \rangle$, $\langle \rho \rangle$.

11) Give the precise Galois correspondence between subgroups of G and intermediate extensions between $\mathbb{Q}$ and N.

Exercise 8.10. Linear independence of $\sqrt{p_k}$ for prime numbers p_k

Set $K = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

1) Show that $\sqrt{5}$ is of degree 2 over K, by comparing $\mathbb{Q}[\sqrt{5}]$ to the intermediate extensions between $\mathbb{Q}$ and K.

Set $L = \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$.

2) Show that L is a normal extension of $\mathbb{Q}$.

3) Determine the structure of the Galois group $G' = \mathrm{Gal}(L|\mathbb{Q})$ (recall that a group all of whose non-trivial elements are of order 2 is isomorphic to a product of groups isomorphic to $\mathbb{Z}/2\mathbb{Z}$; this result follows if one considers the group as a $\mathbb{Z}/2\mathbb{Z}$-vector space).

4) Let us admit the fact that G' has seven subgroups of index 2 (they are hyperplanes for the $\mathbb{Z}/2\mathbb{Z}$-vector space structure, and there are as many of them as there are independent non-zero vectors in the dual of this vector space). Find the set of quadratic extensions of $\mathbb{Q}$ contained in L.

5) Generalize the above to extensions of $\mathbb{Q}$ by $\{\sqrt{p}; p \in E\}$, where E is a finite subset of the set of prime numbers.

COMMENTARY. – By results of Besicovitch and J. Richard (see the book by Gaal), this result can be generalized to a finite set of n-th roots of distinct prime numbers.

Solutions to Some of the Exercises

Solution to Exercise 8.3. $G = \{\text{id}\}$ since the $\mathbb{Q}$-algebra L is generated by $\sqrt[3]{2}$ and $\sqrt[5]{3}$, and a $\mathbb{Q}$-automorphism of L leaves them fixed since their other conjugates are not real, so do not lie in L. The Galois correspondence does not hold in this situation since L has non-trivial subextensions, namely $\mathbb{Q}[\sqrt[3]{2}], \mathbb{Q}[\sqrt[5]{3}]$, whereas G has no non-trivial subgroups.

Solution to Exercise 8.4.

1) $X^2 - 2$ has splitting field $\mathbb{Q}[\sqrt{2}]$ over $\mathbb{Q}$. As this extension is of degree 2 over $\mathbb{Q}$, the group $\text{Gal}(\mathbb{Q}[\sqrt{2}]|\mathbb{Q})$ has two elements, the identity on $\mathbb{Q}[\sqrt{2}]$ and the element $\sigma : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{2}]$ defined by $\sigma(\sqrt{2}) = -\sqrt{2}$. This group is thus isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and has only trivial subgroups. Thus, there is no intermediate extension between $\mathbb{Q}$ and $\mathbb{Q}[\sqrt{2}]$, which we could have noted directly by considering degrees. So we obtain $G \simeq S_2$.

2) $(X^2-2)(X^2-3)$ has splitting field $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ over $\mathbb{Q}$. As this extension is of degree 4 over $\mathbb{Q}$, we find that $G = \text{Gal}(\mathbb{Q}[\sqrt{2}, \sqrt{3}]|\mathbb{Q})$ has four elements; thus it is isomorphic to either $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. To decide which of these is the right group, we need to study G; its elements σ_1, σ_2, σ_3, σ_4 are extensions of $\mathbb{Q}$-automorphisms of $\mathbb{Q}[\sqrt{2}]$. They are are defined by the images of $\sqrt{2}$ and $\sqrt{3}$, and these images are conjugates, so they must be equal to $\pm\sqrt{2}$ and $\pm\sqrt{3}$ (Table 8.4).

	$\sqrt{2}$	$\sqrt{3}$
σ_1	$\sqrt{2}$	$\sqrt{3}$
σ_2	$-\sqrt{2}$	$\sqrt{3}$
σ_3	$\sqrt{2}$	$-\sqrt{3}$
σ_4	$-\sqrt{2}$	$-\sqrt{3}$

TABLE 8.4.

We see that the element σ_1 is of course the identity element, and σ_2, σ_3, σ_4 are of order two. Thus G is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; its subgroups are $\{\sigma_1\}$, $\langle\sigma_2\rangle$, $\langle\sigma_3\rangle$, $\langle\sigma_4\rangle$, and G. The corresponding fields of invariants are

$\mathbb{Q}[\sqrt{2},\sqrt{3}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{6}]$ and $\mathbb{Q}$. We can guess these intermediate extensions easily and check that they work: for example, $\mathbb{Q}[\sqrt{3}]$ is invariant under $\langle\sigma_2\rangle$ and its degree is equal to the index of $\langle\sigma_2\rangle$ in G. Without this intuition, we would need to work with a basis of $\mathbb{Q}[\sqrt{2},\sqrt{3}]$ over $\mathbb{Q}$, for example $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$, and solve the equations $x = \sigma_i(x)$, $i = 2, 3, 4$, with $x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$.

The factorizations of $(X^2-2)(X^2-3)$ are given by
$(X-\sqrt{2})(X+\sqrt{2})(X^2-3)$ over $\mathbb{Q}[\sqrt{2}]$;
$(X-\sqrt{3})(X+\sqrt{3})(X^2-2)$ over $\mathbb{Q}[\sqrt{3}]$;
$(X^2-2)(X^2-3)$ over $\mathbb{Q}[\sqrt{6}]$.

Choosing the correspondence defined in Table 8.5, we obtain the elements of the subgroup of S_4 isomorphic to G (Table 8.6).

$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{3}$	$-\sqrt{3}$
1	2	3	4

TABLE 8.5.

σ_1	σ_2	σ_3	σ_4
id	(1 2)	(3 4)	(1 2)(3 4)

TABLE 8.6.

3) X^3-1 has splitting field $\mathbb{Q}[j]$ over $\mathbb{Q}$, and we can reason exactly as in part **1)**.

4) X^3+2 has the same splitting field over $\mathbb{Q}$ as X^3-2, since its roots are the negatives of the roots of X^3-2. So we can reason as in §8.3 and §8.6.

5) We saw (Exercise 7.1) that the splitting field of X^4+1 over $\mathbb{Q}$ is $N = \mathbb{Q}[\zeta] = \mathbb{Q}[i,\sqrt{2}]$ with $\zeta = e^{i\pi/4} = (1+i)/\sqrt{2}$. We find the intermediate extensions $\mathbb{Q}[i], \mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[i\sqrt{2}]$ by the same procedure as in **2)**, and the elements of the Galois group are defined by Table 8.7.

	i	$\sqrt{2}$	ζ	ζ^3	ζ^5	ζ^7
σ_1	i	$\sqrt{2}$	ζ	ζ^3	ζ^5	ζ^7
σ_2	$-i$	$\sqrt{2}$	ζ^7	ζ^5	ζ^3	ζ
σ_3	i	$-\sqrt{2}$	ζ^5	ζ^7	ζ	ζ^3
σ_4	$-i$	$-\sqrt{2}$	ζ^3	ζ	ζ^7	ζ^5

TABLE 8.7.

The factorizations of X^4+1 over an intermediate extension L are obtained by regrouping the roots of X^4+1,which are conjugates over L. To compute the action of G on these roots, it is useful to add columns giving their images to Table 8.7; for example, the conjugate of ζ over $\mathbb{Q}[i]$ is $\sigma_3(\zeta)=\zeta^5$, etc. The factorizations of X^4+1 follow from this:

- over $\mathbb{Q}[i]$:

$$[(X-\zeta)(X-\zeta^5)][(X-\zeta^3)(X-\zeta^7)]=(X^2-i)(X^2+i);$$

- over $\mathbb{Q}[\sqrt{2}]$:

$$[(X-\zeta)(X-\zeta^7)][(X-\zeta^3)(X-\zeta^5)]=(X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1);$$

- over $\mathbb{Q}[i\sqrt{2}]$:

$$[(X-\zeta)(X-\zeta^3)][(X-\zeta^5)(X-\zeta^7)]=(X^2-i\sqrt{2}X-1)(X^2+i\sqrt{2}X-1).$$

6) X^4-1 has splitting field $\mathbb{Q}[i]$ over $\mathbb{Q}$; the solution works exactly as in **1)**. By numbering the numbers $1,-1,i,-i$ as 1, 2, 3, 4, we identify the group G with the subgroup of S_4 given by id and (34).

Solution to Exercise 8.5.

1) The quotient $\mathrm{Gal}(N|K)/H$ is not necessarily a group, but it is a coset space of order $|\mathrm{Gal}(N|K)|/|H|=[N:K]/[N:I(H)]=[I(H):K]$.

2) The number of K-homomorphisms from L to $\mathbb{C}$ is equal to $[L:K]$, so the number of K-automorphisms of L is $\leq[L:K]$. If we have equality, this means that $\sigma(L)\subset L$ for every K-homomorphism σ of L in $\mathbb{C}$, which in turn means that L is a normal extension of K.

3) The different factors do not bring any more information than does the first. Examples: $\prod_{1\leq k\leq n}(X^2+k^2)$ whose splitting field is $\mathbb{Q}[i]$, $\prod_{1\leq k\leq n}(X^2-2k^2)$ whose splitting field is $\mathbb{Q}[\sqrt{2}]$, etc.

4) Assume that P and Q are relatively prime. If $P(X+a)/Q(X+a)=P(X)/Q(X)$, we have

$$P(X+a)Q(X)=P(X)Q(X+a).$$

$P(X)$, which is relatively prime to $Q(X)$, divides $P(X+a)$, so that we have $P(X+a)=\lambda P(X)$. Comparing the highest degree terms implies that

$\lambda = 1$; if $\deg(P) = n \geq 1$, then comparing the terms of degree $n-1$ gives a contradiction for $a \neq 0$.

Solution to Exercise 8.6.

1) If $L' \cup L''$ generates N, $\sup(L', L'') = N$ in the trellis of extensions, so $\inf(G', G'') = \{\mathrm{id}\}$, i.e. $G' \cap G'' = \{\mathrm{id}\}$.

If $L' \cap L'' = K$, then $\inf(L', L'') = K$ in the trellis of extensions, so $\sup(G', G'') = G$, i.e. G' and G'' generate G.

If L and L' are normal extensions of K, then G' and G'' are normal subgroups of G.

These three conditions imply that $G \simeq G' \times G''$.

2) The converse is shown simply by running the argument backward.

3) The first question asserts that $\mathrm{Gal}(N|K) \simeq \mathrm{Gal}(N|L') \times \mathrm{Gal}(N|L'')$. Proposition 8.4 shows that we have both $\mathrm{Gal}(N|K)/\mathrm{Gal}(N|L') \simeq \mathrm{Gal}(L'|K)$ and $\mathrm{Gal}(N|K)/\mathrm{Gal}(N|L'') \simeq \mathrm{Gal}(L''|K)$. It follows that $\mathrm{Gal}(N|L') \simeq \mathrm{Gal}(L''|K)$ and $\mathrm{Gal}(N|L'') \simeq \mathrm{Gal}(L'|K)$, which gives the result.

Solution to Exercise 8.7.

1) If a, b, c lie in K, then $G = \{\mathrm{id}\}$ and $d \in K$. If a and b are of degree 2 and conjugate over K, then c lies in K, $d \notin K$ and $G \simeq \mathbb{Z}/2\mathbb{Z}$.

2) a) If $d \in K$, $[K[a,b,c] : K] = [K[a,d] : K] = 3$ so $G \simeq \mathbb{Z}/3\mathbb{Z}$, and there is no non-trivial intermediate extension.

If d is of degree 2 over K, then $[K[d] : K] = 2$ and $[K[a] : K] = 3$, so that $[K[a,b,c] : K] = 6$. Thus G is of order 6. As G is isomorphic to a subgroup of S_3, it must be isomorphic to S_3. There are four intermediate extensions corresponding to the four non-trivial subgroups of S_3. The one of degree 2 is $K[d]$. The ones of degree 3 are $K[a]$, $K[b]$ and $K[c]$. The elements of G are given in Table 8.8.

	a	b	c	d
σ_1	a	b	c	d
σ_2	b	c	a	d
σ_3	c	a	b	d
σ_4	a	c	b	$-d$
σ_5	c	b	a	$-d$
σ_6	b	a	c	$-d$

TABLE 8.8.

3) a) As $X^3-2X-1=(X+1)(X^2-X-1)$, we see that the splitting field of X^3-2X-1 is $\mathbb{Q}[\sqrt{5}]$; its Galois group over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, and its Galois group over $\mathbb{Q}[\sqrt{5}]$ is trivial.

b) As X^3-3X+1 is irreducible over $\mathbb{Q}$ (the possible rational roots, namely ± 1, do not work), and moreover $D=9^2$, we find that $G\simeq\mathbb{Z}/3\mathbb{Z}$.

c) Similarly, X^3-4X+1 is irreducible over $\mathbb{Q}$ and, as $D=229$ is not a square in $\mathbb{Q}$, we have $G\simeq S_3$.

d) X^3-2X+2 is irreducible over $\mathbb{Q}$ (use Eisenstein's criterion); consequently, it is also irreducible over $= QQ[i\sqrt{19}]$. As $D=-76$, its Galois group over $\mathbb{Q}$ is isomorphic to S_3, and its Galois group over $\mathbb{Q}[i\sqrt{19}]$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$.

e) X^3-5 is irreducible over $\mathbb{Q}$ and $\mathbb{Q}[i\sqrt{3}]$; as its discriminant is $D=-3\times 15^2$, its Galois group over $\mathbb{Q}$ is isomorphic to S_3 and its Galois group over $\mathbb{Q}[i\sqrt{3}]$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$. Over $\mathbb{Q}[\sqrt[3]{5}]$, X^3-5 is reducible and its Galois group is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

f) The polynomial factors as $(X^2+3)(X^3-3X+1)$. The splitting fields of the two factors are of degrees 2 and 3 over $\mathbb{Q}$, and their Galois groups over $\mathbb{Q}$ are isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ respectively. By Exercise 8.6, the Galois group of X^5+X^2-9X+3 over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\simeq\mathbb{Z}/6\mathbb{Z}$. A generator of this group is the $\mathbb{Q}$-automorphism defined by $\sigma(a)=b$ and $\sigma(i\sqrt{3})=-i\sqrt{3}$, where a and b are two distinct roots of X^3-3X+1.

Solution to Exercise 8.8.

1) a) If $N=K[\sqrt{a},\sqrt{b}]$, then N is the splitting field of the polynomial $(X^2-a)(X^2-b)$ over K, so it is a normal extension of K. The Galois group has four elements, namely the elements $\sigma_1=\mathrm{id}$, σ_2, σ_3 and σ_4 defined in Table 8.9.

	σ_1	σ_2	σ_3	σ_4
$\sqrt{a}$	$\sqrt{a}$	$\sqrt{a}$	$-\sqrt{a}$	$-\sqrt{a}$
$\sqrt{b}$	$\sqrt{b}$	$-\sqrt{b}$	$\sqrt{b}$	$-\sqrt{b}$

TABLE 8.9.

Clearly, G has three elements of order two, so it is isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. The subgroups of order two of G are generated by these three elements. They correspond to three intermediate extensions:

$$I(\langle\sigma_2\rangle)=K[\sqrt{a}],\quad I(\langle\sigma_3\rangle)=K[\sqrt{b}],\quad I(\langle\sigma_4\rangle)=K[\sqrt{ab}].$$

b) Let H_1 and H_2 be two distinct subgroups of order two of $\mathrm{Gal}(N|K)$. The fields $I(H_1)$ and $I(H_2)$ are distinct quadratic extensions of K, so they

generate N; there exist a and $b \in K$ such that $I(H_1) = K[\sqrt{a}]$ and $I(H_2) = K[\sqrt{b}]$ (see Exercise 4.7). Hence $N = K[\sqrt{a}, \sqrt{b}]$.

2) a) Clearly α is a root of the polynomial $P(X) = X^4 - 12X^2 + 25$.

We have $P(X+1) = X^4 + 4X^3 - 6X^2 - 20X + 14$. Applying Eisenstein's criterion with $p = 2$ shows that $P(X+1)$ is irreducible over $\mathbb{Q}$, so $P(X)$ is also irreducible. We can also try to factor P in $\mathbb{Z}[X]$ using Descartes' method, but this turns out to be impossible.

b) As $\sqrt{11} = \alpha^2 - 6$, we have $\mathbb{Q}[\sqrt{11}] \subset \mathbb{Q}[\alpha]$. The inclusion is strict because $\mathbb{Q}[\alpha]$ is an extension of degree 4 of $\mathbb{Q}$ by **a)**. Furthermore, $\alpha\beta = 5$ shows that $\beta = 5/\alpha$; thus β lies in $\mathbb{Q}[\alpha]$. As $\alpha(\alpha^3 - 12\alpha) = -25$, we have $\beta = (12/5)\alpha - (1/5)\alpha^3$.

c) The roots of P are $\pm\alpha$ and $\pm\beta$. As $\beta \in \mathbb{Q}[\alpha]$ by **b)**, $\mathbb{Q}[\alpha]$ is a normal extension of $\mathbb{Q}$.

d) When σ is in G, $\sigma(\alpha)$ is a conjugate of α, so $\sigma(\alpha)$ equals $\pm\alpha$ or $\pm\beta$. The group G contains the four elements $\sigma_1 = \text{id}$, σ_2, σ_3 and σ_4 defined by Table 8.10.

	σ_1	σ_2	σ_3	σ_4
α	α	$-\alpha$	β	$-\beta$
β	β	$-\beta$	α	$-\alpha$

TABLE 8.10.

Since we know that

$$\sigma_2(\sigma_2(\alpha)) = \sigma_2(-\alpha) = \alpha, \qquad \sigma_3(\sigma_3(\alpha)) = \sigma_3(\beta) = \sigma_3\left(\frac{5}{\alpha}\right) = \frac{5}{\beta} = \alpha,$$

and

$$\sigma_4(\sigma_4(\alpha)) = \sigma_4(-\beta) = \sigma_4\left(-\frac{5}{\alpha}\right) = \frac{5}{\beta} = \alpha,$$

we see that G contains three elements of order 2, so it is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/r2\mathbb{Z}$.

e) The conjugates of $\alpha + \beta$ are $\alpha + \beta$ and $\sigma_2(\alpha + \beta) = -\alpha - \beta$. The conjugates of $\alpha - \beta$ are $\alpha - \beta$ and $\sigma_2(\alpha - \beta) = \beta - \alpha$. Thus $\alpha + \beta$ and $\alpha - \beta$ are of degree 2 over $\mathbb{Q}$. We find that $(\alpha + \beta)^2 = 12 + 10 = 22$, $(\alpha - \beta)^2 = 12 - 10 = 2$. But $\alpha + \beta$ and $\alpha - \beta$ are > 0, so $\alpha + \beta = \sqrt{22}$ and $\alpha - \beta = \sqrt{2}$. Finally, we have $\alpha = \sqrt{11/2} + \sqrt{1/2}$ and $\beta = \sqrt{11/2} - \sqrt{1/2}$.

f) The intermediate extensions of degree 2 over $\mathbb{Q}$ are given by

$$I(\langle\sigma_2\rangle) = \mathbb{Q}[\alpha^2] = \mathbb{Q}[\sqrt{11}], \qquad I(\langle\sigma_3\rangle) = \mathbb{Q}[\sqrt{22})], \qquad I(\langle\sigma_4\rangle) = \mathbb{Q}[\sqrt{2}].$$

Solution to Exercise 8.9.

1) We have $D = -4p^3 - 27q^2 = -216$ and $d = 6i\sqrt{6}$. Now, P is a cubic polynomial with real coefficients and negative discriminant, so it has one real root and two complex conjugate roots.

2) Cardan's formulas give $a = u + v$, $b = ju + j^2v$, $c = j^2u + jv$ (the inequalities $u > 0$ and $v < 0$ make it possible to see which of $j^2u + jv$ and $ju + j^2v$ has positive imaginary part).

We check that P is irreducible over $\mathbb{Q}$ by making sure that none of the possible candidates for rational roots works: ± 1 and ± 2 are not roots of P. As -216 is not a square in $\mathbb{Q}$, Γ is isomorphic to S_3.

3) As $u^3 - 1 = \sqrt{2}$, u is algebraic over $\mathbb{Q}[\sqrt{2}]$, so it is algebraic over $\mathbb{Q}$. As $a = u + v$ and $v = -1/u$, we see that $a \in \mathbb{Q}[u]$. Thus $\mathbb{Q}[u]$, which contains the extensions $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[a]$, of degrees 2 and 3 over $\mathbb{Q}$, is of degree a multiple of 6 over $\mathbb{Q}$. The equality $(u^3 - 1)^2 = 2$ shows that u is of degree ≤ 6. We conclude that the degree of u over $\mathbb{Q}$ is equal to 6 and that its minimal polynomial over $\mathbb{Q}$ is given by $X^6 - 2X^3 - 1$.

4) The conjugates of u over $\mathbb{Q}$ are the solutions of $(x^3 - 1)^2 = 2$; we find u, ju, j^2u, v, jv, j^2v. We check that $N \subset \mathbb{Q}[u, j]$ because $v = -1/u$, and that $\mathbb{Q}[u, j] \subset N$ because $j = ju/u$. This gives $N = \mathbb{Q}[u, j]$.

5) We first mention $\mathbb{Q}[a]$, $\mathbb{Q}[b]$, $\mathbb{Q}[c]$, of degree 3 over $\mathbb{Q}$, $\mathbb{Q}[d] = \mathbb{Q}[i\sqrt{6}]$, of degree 2 over $\mathbb{Q}$, and $\mathbb{Q}[a, b, c]$, of degree 6 over $\mathbb{Q}$. Other intermediate extensions are easy to see: $\mathbb{Q}[u]$, of degree 6 over $\mathbb{Q}$. We can also mention $\mathbb{Q}[j, \sqrt{2}]$, of degree 4 over $\mathbb{Q}$, $\mathbb{Q}[ju] = \mathbb{Q}[j^2v]$, $\mathbb{Q}[j^2u] = \mathbb{Q}[jv]$, of degree 6 over $\mathbb{Q}$.

6) As u is real and j is not, j is of degree 2 over $\mathbb{Q}[u]$ and $[N : \mathbb{Q}] = 12$. As N is a normal extension of $\mathbb{Q}$, we have $|G| = [N : \mathbb{Q}] = 12$.

7) We see that $\sigma^2 = \mathrm{id}$ so σ is of order 2. As $uv = -1$, $\rho(uv) = -1$, $\rho(v) = -1/\rho(u) = -1/jv = j^2u$. We can then fill out the first three columns of Table 8.11. We see that ρ is of order 6 and that the 12 elements of G can be written ρ^k and $\rho^k\sigma$ with $0 \leq k \leq 5$. As $\sqrt{2} = u^3 - 1$, $\rho(\sqrt{2}) = (jv)^3 - 1 = -\sqrt{2}$. Finally, we have

$$\sigma(d) = 6\sigma(i\sqrt{3})\sigma(\sqrt{2}) = 6(-i\sqrt{3})(\sqrt{2}) = -d,$$

$$\rho(d) = \rho(6i\sqrt{6}) = 6\rho(i\sqrt{3})\rho(\sqrt{2}) = 6(-i\sqrt{3})(-\sqrt{2}) = d.$$

8) Table 8.11 shows that the $\mathbb{Q}$-automorphisms ρ^k and $\rho^k\sigma$ for $0 \leq k \leq 5$ are all different, so that we have indeed found all the elements of G. Consequently, ρ and σ generate G.

Moreover, $\sigma\rho = \rho^5\sigma$, as it is easy to check on u and j. With the relations $\rho^6 = \sigma^2 = \mathrm{id}$, this shows that G is isomorphic to the dihedral group D_6.

9) As $[\mathbb{Q}[u] : \mathbb{Q}] = 6$, $\mathrm{Gal}(N|\mathbb{Q}[u])$ has two elements. Table 8.11 shows that these are exactly id and σ. As $\mathbb{Q}[u]$ is not a normal extension of $\mathbb{Q}$, this subgroup is not normal in G.

10) $\langle \sigma, \rho^2 \rangle$ has six elements: id, ρ^2, ρ^4, σ, $\rho^2\sigma$ and $\rho^4\sigma$, so we are looking for a quadratic extension of $\mathbb{Q}$. Table 8.11 shows that it is given by $\mathbb{Q}[\sqrt{2}]$.

$\langle \rho\sigma, \rho^2 \rangle$ has six elements: id, ρ^2, ρ^4, $\rho\sigma$, $\rho^3\sigma$ and $\rho^5\sigma$, so we are looking for a quadratic extension of $\mathbb{Q}$. Table 8.11 shows that it is given by $\mathbb{Q}[j]$.

$\langle \rho \rangle$ has six elements, so we are looking for a quadratic extension of $\mathbb{Q}$. Table 8.11 shows that it is $\mathbb{Q}[d]$.

	u	j	v	$\sqrt{2}$	d	a, b, c
id	u	j	v	$\sqrt{2}$	d	a, b, c
ρ	jv	j^2	j^2u	$-\sqrt{2}$	d	c, a, b
ρ^2	ju	j	j^2v	$\sqrt{2}$	d	b, c, a
ρ^3	v	j^2	u	$-\sqrt{2}$	d	a, b, c
ρ^4	j^2u	j	jv	$\sqrt{2}$	d	c, a, b
ρ^5	j^2v	j^2	ju	$-\sqrt{2}$	d	b, c, a
σ	u	j^2	v	$\sqrt{2}$	$-d$	a, c, b
$\rho\sigma$	jv	j	j^2u	$-\sqrt{2}$	$-d$	c, b, a
$\rho^2\sigma$	ju	j^2	j^2v	$\sqrt{2}$	$-d$	b, a, c
$\rho^3\sigma$	v	j	u	$-\sqrt{2}$	$-d$	a, c, b
$\rho^4\sigma$	j^2u	j^2	jv	$\sqrt{2}$	$-d$	c, b, a
$\rho^5\sigma$	j^2v	j	ju	$-\sqrt{2}$	$-d$	b, a, c

TABLE 8.11.

11) An isomorphism of G with D_6 is given by associating to ρ the rotation r of angle $\pi/3$ and center O, and to $\rho^k\sigma$ the symmetry $r^k s$ with respect to the line making an angle of $k\pi/6$ with (OA).

This isomorphism gives the list of subgroups of G by making the list of subgroups of D_6, which is easier thanks to geometric considerations.

Subgroups with two elements

These subgroups are generated by elements of order 2 and correspond to the symmetries with respect to O or with respect to lines. We find: $H_1 = \langle \rho^3 \rangle$, $H_{k+2} = \langle \rho^k\sigma \rangle$ with $0 \leq k \leq 5$.

Subgroups with four elements

As there is no element of order 4, these subgroups all correspond to the subgroups of D_6 generated by symmetries with respect to two perpendicular axes (which thus commute).

They are given by $H_8 = \langle \sigma, \rho^3\sigma \rangle$, $H_9 = \langle \rho\sigma, \rho^4\sigma \rangle$, $H_{10} = \langle \rho^2\sigma, \rho^5\sigma \rangle$; they all contain ρ^3.

Subgroups with three elements
The only such subgroup is given by $H_{11} = \langle \rho^2 \rangle$, because the only elements of order 3 in D_6 are ρ^2 and ρ^4.

Subgroups with six elements
As ρ and ρ^5 are the only elements of order 6, $H_{12} = \langle \rho \rangle$ is a cyclic subgroup of order 6. If there are other subgroups with six elements, they are isomorphic to S_3, which is isomorphic to D_3, the dihedral group of isometries of an equilateral triangle. There are two ways of placing an equilateral triangle with center O with respect to the hexagon: a vertex at A or the rotation of this by $\pi/6$. Thus we find two other subgroups of G of order 6:

$$\begin{aligned} H_{13} &= \{\mathrm{id}, \sigma, \rho^2\sigma, \rho^4\sigma, \rho^2, \rho^4\} = \langle \sigma, \rho^2 \rangle \\ H_{14} &= \{\mathrm{id}, \rho\sigma, \rho^3\sigma, \rho^5\sigma, \rho^2, \rho^4\} = \langle \rho\sigma, \rho^2 \rangle. \end{aligned}$$

Let L_i denote the extension corresponding to the subgroup H_i, $1 \le i \le 14$. To find L_i, we will look for an extension L invariant under H_i (so $L \subset L_i$) of suitable degree: $[L_i : \mathbb{Q}] = [N : \mathbb{Q}]/[N : L_i] = |G|/|H_i|$.

Among the subgroups of G, only H_1, H_{11}, H_{12}, H_{13}, and H_{14} are normal; the corresponding extensions are thus normal extensions of $\mathbb{Q}$. It is useful to add a column to Table 8.11 to describe the action of the elements of G on the roots a, b, c of P. We find that

$$\begin{aligned} L_1 &= \mathbb{Q}[a,d] = \mathbb{Q}[a,b,c], & L_2 &= \mathbb{Q}[u] = \mathbb{Q}[v] = \mathbb{Q}[a,\sqrt{2}], \\ L_3 &= \mathbb{Q}[b,j], & L_4 &= \mathbb{Q}[j^2u] = \mathbb{Q}[c,\sqrt{2}], \\ L_5 &= \mathbb{Q}[a,j], & L_6 &= \mathbb{Q}[ju] = \mathbb{Q}[b,\sqrt{2}], \\ L_7 &= \mathbb{Q}[c,j], & L_8 &= \mathbb{Q}[a], \\ L_9 &= \mathbb{Q}[b], & L_{10} &= \mathbb{Q}[c], \\ L_{11} &= \mathbb{Q}[j,d] = \mathbb{Q}[j,\sqrt{2}], & L_{12} &= \mathbb{Q}[d] = \mathbb{Q}[i\sqrt{6}], \\ L_{13} &= \mathbb{Q}[\sqrt{2}], & L_{14} &= \mathbb{Q}[j] = \mathbb{Q}[i\sqrt{3}]. \end{aligned}$$

Solution to Exercise 8.10.

1) If $\sqrt{5} \in K$, then $\mathbb{Q}[\sqrt{5}]$ is one of the three intermediate extensions $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{6}]$, but it is easily seen that this is impossible.

2) L is the splitting field of $(X^2-2)(X^2-3)(X^2-5)$ over $\mathbb{Q}$.

3) As $[L : \mathbb{Q}] = 8$, the order of G' is 8, so $G' \simeq (\mathbb{Z}/2\mathbb{Z})^3$.

4) The complete list is easy to establish: $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{5}]$, $\mathbb{Q}[\sqrt{6}]$, $\mathbb{Q}[\sqrt{10}]$, $\mathbb{Q}[\sqrt{15}]$, $\mathbb{Q}[\sqrt{30}]$.

5) We use induction on the cardinal n of E, and show that $\mathbb{Q}[\{\sqrt{p}; p \in E\}]$ is an extension of $\mathbb{Q}$ of degree 2^n and Galois group $(\mathbb{Z}/2\mathbb{Z})^n$, in which $\{\sqrt{p}; p \in E\}$ is a free system over $\mathbb{Q}$. The result is obvious if $n = 1$. Assume it holds for some integer $n \geq 1$, and let E have cardinal $n+1$. If $p_1 \in E$, then we apply the induction hypothesis to $E - \{p_1\}$. The field $\mathbb{Q}\left[\{\sqrt{p}, p \in E, p \neq p_1\}\right]$ has $2^n - 1$ quadratic subextensions, given by the $\mathbb{Q}\left[\prod_{p \in F} \sqrt{p}\right]$ for non-empty subsets F of $E - \{p_1\}$, and none of these extensions is equal to $\mathbb{Q}[\sqrt{p_1}]$. This concludes the proof.

9
Roots of Unity

In this chapter, we give the first example of a family of extensions whose Galois group is actually computable: this is the family of extensions of a field by roots of unity. The earliest work on this subject is due to Vandermonde (1770). It was followed by work of Gauss, in particular his beautiful discovery, on March 30, 1796, at the age of 19, of the construction of the regular polygon with 17 sides with ruler and compass (see Exercise 9.7) and its consequences.

9.1 The Group $U(n)$ of Units of the Ring $\mathbf{Z}/n\mathbf{Z}$

9.1.1 Definition and Background

The invertible elements of a ring A are often called *units*; they form a group under the multiplication law of A.

Let n be an integer > 1. The *group of units* of the ring $\mathbb{Z}/n\mathbb{Z}$ is written $U(n)$. The map associating the order of the group $U(n)$ to the integer n is written φ and called the *Euler function.* Euler introduced it in 1760, to generalize results of Fermat, and proved the statements 2) and 4) of Proposition 9.1.2 below. In our notation, we make no distinction between an integer and its class modulo n.

Recall that k is invertible in $U(n)$ if and only if k is relatively prime to n. Indeed, if k is prime to n, Bézout's identity gives integers u and v such that $uk + vn = 1$, so that $uk = 1$ in $U(n)$, and if k is not prime to n,

there exist $d, u, v \neq 0$ mod n such that $k = ud, n = vd$. Because $kv = 0$ in $U(n)$, k is not invertible in $U(n)$.

EXAMPLES. –

1) The underlying set of the group $U(8)$ is $\{1, 3, 5, 7\}$, and we have $\varphi(8) = 4$. Its elements are all of order 2, so we have $U(8) \simeq (\mathbb{Z}/2\mathbb{Z})^2$.

2) The underlying set of the group $U(15)$ is $\{1, 2, 4, 7, 8, 11, 13, 14\}$, so $\varphi(15) = 8$. Its elements are of order 2 or 4, which is the case for exactly one of the three abelian groups of order 8, so we know that $U(8) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Fortunately, there exists a general theorem giving the structure of the group $U(n)$.

9.1.2 The Structure of U(n)

PROPOSITION. – *The group $U(n)$ is abelian. Moreover:*

1) If $n = rs$ where r and s are relatively prime, we have $U(n) \simeq U(r) \times U(s)$ and $\varphi(n) = \varphi(r)\varphi(s)$.

2) If $n = p^k$, where p is a prime greater than 2, then $U(n)$ is cyclic of order $\varphi(p^k) = p^k - p^{k-1}$.

3) For $k \geq 2$, we have $U(2^k) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$; for $k = 1$, we have $U(2) \simeq \{0\}$.

4) If $\{p_i; i \in I\}$ is the set of distinct prime factors of n, we have $\varphi(n) = n \prod_{i \in I}(1 - \frac{1}{p_i})$.

PROOF. – The proof is entirely given in the exercises (see Exercise 9.8). ◇

EXAMPLE. – We have $2,800 = 16 \times 25 \times 7$, so

$$\begin{aligned} U(2,800) &\simeq U(16) \times U(25) \times U(7) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \\ \varphi(2,800) &= 2,800\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right) = 960. \end{aligned}$$

9.2 The Möbius Function

Let $D(n)$ denote the set of divisors of n.

9.2.1 Multiplicative Functions

DEFINITION. – A function $f : \mathbb{N}^* \to \mathbb{Z}$ (or $\mathbb{R}$) is called *multiplicative* if for every pair (m, n) of relatively prime numbers, we have $f(mn) = f(m)f(n)$.

EXAMPLE. – The Euler function is a multiplicative function by §9.1.2.

9.2.2 The Möbius Function

Let $\mu : \mathbb{N} \to \mathbb{Z}$ denote the function, known as the *Möbius function*, defined by

$$\begin{aligned} \mu(1) &= 1, \\ \mu(n) &= 0 \text{ if } n \text{ has a square factor}, \\ \mu(n) &= (-1)^r \text{ if } n \text{ is a product of } r \text{ distinct primes.} \end{aligned}$$

9.2.3 Proposition

The Möbius function is a multiplicative function, and for all $n > 1$, we have

$$\sum_{d \in D(n)} \mu(d) = 0.$$

PROOF. – If m and n are relatively prime integers, then either one of them has a square factor or neither one does. In both cases, we check that $\mu(mn) = \mu(m)\mu(n)$.

If

$$n = \prod_{i \in \{1,\ldots,r\}} (p_i)^{k_i}$$

is the decomposition of n into a product of distinct primes, and if $m = \prod_{i \in \{1,\ldots,r\}} p_i$, we have

$$\sum_{d \in D(n)} \mu(d) = \sum_{d \in D(m)} \mu(d) = \sum_{0 \le k \le r} \binom{r}{k} (-1)^k,$$

which is the expansion of $(1-1)^r = 0$. ◇

9.2.4 The Möbius Inversion Formula

PROPOSITION. – *Let G be an abelian group written additively. Let $g : \mathbb{N}^* \to G$ be a map, and let $f : \mathbb{N}^* \to G$ be the map defined by $f(n) = \sum_{d\in D(n)} g(d)$. Then*

$$g(n) = \sum_{d\in D(n)} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d\in D(n)} \mu\left(\frac{n}{d}\right) f(d).$$

REMARK. – If the group law of G is written multiplicatively, then f is defined by $f(n) = \prod_{d\in D(n)} g(d)$ and the inversion formula is written as

$$g(n) = \prod_{d\in D(n)} f\left(\frac{n}{d}\right)^{\mu(d)} = \prod_{d\in D(n)} f(d)^{\mu(n/d)}.$$

PROOF. – Let us give a direct proof. We have

$$\begin{aligned}\sum_{d\in D(n)} \mu(d) f\left(\frac{n}{d}\right) &= \sum_{d\in D(n)} \left(\mu(d) \sum_{e\in D(n/d)} g(e)\right) \\ &= \sum_{e\in D(n)} \left(g(e) \sum_{d\in D(n), e\in D(n/d)} \mu(d)\right).\end{aligned}$$

For every $e \in D(n)$, we have

$$\left\{d; d \in D(n) \text{ and } e \in D\left(\frac{n}{d}\right)\right\} = \left\{d; d \in D(n) \text{ and } d \in D\left(\frac{n}{e}\right)\right\} = D\left(\frac{n}{e}\right),$$

so we have

$$\sum_{d\in D(n)} \mu(d) f\left(\frac{n}{d}\right) = \sum_{e\in D(n)} \left(g(e) \sum_{d\in D(n/e)} \mu(d)\right) = g(n)$$

since $\sum_{d\in D(n/e)} \mu(d) = 0$ for $e < n$ by the formula of Proposition 9.2.3. ◇

COMMENTARY. – August Möbius is better known for his band, or for the invention of barycenters. He introduced his function in 1832, using it for an inversion formula that was generalized independently by Dedekind and by Liouville in 1857.

9.3 Roots of Unity

9.3.1 n-th Roots of Unity

DEFINITION. – Let $n > 1$ be an integer. An n-th root of unity in $\mathbb{C}$ is a complex number ζ such that $\zeta^n = 1$. Any such ζ is of the form $\zeta = \mathrm{e}^{2ik\pi/n}$ for some integer k with $0 \leq k < n$.

9.3.2 Proposition

The set of n-th roots of unity in $\mathbb{C}$ forms a cyclic group μ_n isomorphic to $(\mathbb{Z}/n\mathbb{Z}, +)$.

PROOF. – Consider the group homomorphism $f : (\mathbb{Z}, +) \to \mathbb{C}^*$ defined by $f(k) = \mathrm{e}^{2ik\pi/n}$. The kernel of this homomorphism is exactly $n\mathbb{Z}$, and its image is μ_n, which gives the result. ◇

9.3.3 Primitive Roots

DEFINITION. – Let $n > 1$ be an integer. A *primitive n-th root of unity* in $\mathbb{C}$ is a generator of the cyclic group μ_n.

9.3.4 Properties of Primitive Roots

Using the isomorphism defined by f above, we see that the primitive n-th roots of unity are of the form $\mathrm{e}^{2ik\pi/n}$ with $1 \leq k < n$ and k prime to n, since the generators of $(\mathbb{Z}/n\mathbb{Z}, +)$ are the classes of integers relatively prime to n. Thus, there exist $\varphi(n)$ primitive n-th roots of unity in $\mathbb{C}$.

If ζ and ζ' are two primitive n-th roots of unity, there exists u prime to n such that $\zeta' = \zeta^u$.

9.4 Cyclotomic Polynomials

9.4.1 Definition

The *n-th cyclotomic polynomial* is the polynomial Φ_n defined by the following expression:

$$\Phi_n(X) = \prod_{\zeta \in \mu_n,\ \zeta \text{ primitive}} (X - \zeta).$$

9.4.2 Properties of the Cyclotomic Polynomial

We will show how to compute Φ_n, and prove that Φ_n is the minimal polynomial of every primitive n-th root of unity in $\mathbb{C}$.

The fact that Φ_n is irreducible over $\mathbb{Q}$ whenever n is prime was proved by Gauss in No. 341 of his *Recherches arithmétiques*, after the definition of the cyclotomic polynomial in No. 339 (Figure 9.1). His proof is not as rapid as the proof using Eisenstein's criterion.

339. L'équation $x^n - 1 = 0$ (en supposant, comme il faut toujours le faire par la suite, que n est un nombre premier impair), ne renferme qu'une seule racine réelle $x = 1$; les $n - 1$ autres, qui sont donnés par l'équation

$$x^{n-1} + x^{n-2} + \text{etc.} + x + 1 = 0, \ldots\ldots (X)$$

sont toutes imaginaires;

341. Théorème. ***Si la fonction X (n° 339) est divisible par une fonction d'un degré inférieur***

$$P = x^{\lambda} + Ax^{\lambda-1} + Bx^{\lambda-2} + \text{etc.} + Kx + L;$$

les coefficiens A, B, ... L ne peuvent pas être tous entiers ni rationnels.

FIGURE 9.1. Articles 339 and 341 of *Recherches arithmétiques*

The irreducibility of Φ_n over $\mathbb{Q}$ for non-prime n was proven by Gauss somewhat later, in 1808. This problem was studied more deeply by several 19th-century mathematicians: Eisenstein, Dedekind, Kronecker, etc.

Proposition. – *For every $n \geq 1$, we have*

1) $X^n - 1 = \prod_{d \in D(n)} \Phi_d(X)$

2) $\Phi_n(X) = \prod_{d \in D(n)} (X^d - 1)^{\mu(n/d)}$, *and when p is a prime, we have*

$$\Phi_p(X) = \sum_{0 \leq k \leq p-1} X^k$$

3) $\Phi_n(X) \in \mathbb{Z}[X]$

4) $\Phi_n(X)$ *is irreducible over* $\mathbb{Q}$.

Proof. –

1) We compute

$$X^n - 1 = \prod_{\zeta \in \mu_n} (X - \zeta) = \prod_{d \in D(n)} \prod_{\zeta \in \mu_n,\ \zeta \text{ of order d}} (X - \zeta)$$

$$= \prod_{d \in D(n)} \prod_{\zeta \in \mu_d,\ \zeta \text{ primitive}} (X - \zeta) = \prod_{d \in D(n)} \Phi_d(X).$$

2) Consider the multiplicative group $G = \mathbb{C}(X)^*$ of non-zero rational functions in one indeterminate with complex coefficients. Let $f, g : \mathbb{N}^* \to G$ be the maps defined by $f(n) = X^n - 1$ and $g(n) = \Phi_n(X)$. By 1), $f(n) = \prod_{d \in D(n)} g(d)$ and the multiplicative form of the Möbius inversion formula gives the result.

3) In the preceding formula, the exponents of the polynomials belong to $\{0, 1, -1\}$; thus $\Phi_n(X)$ is a polynomial which is the quotient of two monic polynomials in $\mathbb{Z}[X]$, which means that it lies in $\mathbb{Z}[X]$.

4) Let ω be a primitive n-th root of unity, and let P be its minimal polynomial over $\mathbb{Q}$. Let E be the set of roots of P in $\mathbb{C}$, and let F be the set of primitive n-th roots of unity. Let us show that $E = F$.

Because $\Phi_n(\omega) = 0$, we see that P divides Φ_n, so $E \subset F$.

To prove the converse inclusion, we first show that E is stable under raising to p-th powers whenever p is a prime not dividing n.

To show this, suppose it is not the case, so there exists an element $\alpha \in E$ and a prime p not dividing n such that $\alpha^p \notin E$. Let S be the polynomial such that $X^n - 1 = P(X)S(X)$. As $\alpha^p \notin E$, $P(\alpha^p) \neq 0$, so $S(\alpha^p) = 0$, which shows that α is a root of $S(X^p)$. As P is the minimal polynomial of α, it divides $S(X^p)$. Set $S(X^p) = P(X)T(X)$. The polynomials S and T lie in $\mathbb{Z}[X]$, since P is monic. We now consider the situation in $(\mathbb{Z}/p\mathbb{Z})[X]$, adding a subscript 1 to denote the images of polynomials of $\mathbb{Z}[X]$ in $(\mathbb{Z}/p\mathbb{Z})[X]$. We have $S_1(X^p) = (S_1(X))^p = P_1(X)T_1(X)$ (to see why, consult §14.4.2). As $(\mathbb{Z}/p\mathbb{Z})[X]$ is a factorial ring, every irreducible factor U_1 of P_1 divides S_1; the equality $X^n - 1 = P_1(X)S_1(X)$ shows that $(U_1)^2$ divides $X^n - 1$; it follows that U_1 divides the derivative nX^{n-1} of $X^n - 1$ in $(\mathbb{Z}/p\mathbb{Z})[X]$. As p is prime to n, these two polynomials are relatively prime in $(\mathbb{Z}/p\mathbb{Z})[X]$, which is a contradiction.

Now, we can finish the proof that $F \subset E$. Let $\zeta \in F$; there exists a number u prime to n such that $\zeta = \omega^u$. Let $u = \prod_{1 \le i \le r} (p_i)^{k_i}$ be the decomposition of u as a product of prime factors. The fact that E is stable under raising to p-th powers whenever p is a prime not dividing n shows that $\alpha = \omega^u = (\ldots(\omega^{p_1})\ldots)^{p_r}$ lies in E. Thus, we have $E = F$, so $\Phi_n = P$, and Φ_n is irreducible over $\mathbb{Q}$. ◇

EXAMPLE. –

$$\begin{aligned}\Phi_{28}(X) &= \prod_{d\in D(28)} (X^d-1)^{\mu(28/d)}\\ &= (X^{28}-1)^{\mu(1)}(X^{14}-1)^{\mu(2)}(X^7-1)^{\mu(4)}(X^4-1)^{\mu(7)}\\ &\quad \cdot(X^2-1)^{\mu(14)}(X-1)^{\mu(28)}\\ &= (X^{28}-1)(X^{14}-1)^{-1}(X^7-1)^0(X^4-1)^{-1}(X^2-1)(X-1)^0\\ &= \frac{(X^{28}-1)(X^2-1)}{(X^{14}-1)(X^4-1)}\\ &= \frac{(X^{14}+1)}{(X^2+1)}\\ &= X^{12}-X^{10}+X^8-X^6+X^4-X^2+1.\end{aligned}$$

A quicker way of computing the cyclotomic polynomials is given in Exercise 9.4.

9.5 The Galois Group over $\mathbf{Q}$ of an Extension of $\mathbf{Q}$ by a Root of Unity

PROPOSITION. – *Let $n \geq 2$ be an integer and ζ a primitive n-th root of unity in $\mathbb{C}$. Then*

1) $\mathbb{Q}[\zeta]$ *is a normal extension of ζ;*

2) $[\mathbb{Q}[\zeta]:\mathbb{Q}] = \varphi(n)$*;*

3) $\mathrm{Gal}(\mathbb{Q}[\zeta]|\mathbb{Q}) \simeq U(n)$*; in particular, this group is abelian.*

PROOF. –

1) Indeed, $\mathbb{Q}[\zeta]$ is the splitting field of X^n-1, or of Φ_n, over $\mathbb{Q}$.

2) The minimal polynomial of ζ over $\mathbb{Q}$ is Φ_n, which is of degree $\varphi(n)$.

3) Set $G = \mathrm{Gal}(\mathbb{Q}[\zeta]|\mathbb{Q})$ and let $\sigma \in G$; then σ is determined by $\sigma(\zeta)$ which is a conjugate of ζ and therefore a primitive n-th root of unity. Thus, it is of the form ζ^k for some k prime to n. We use this k to construct a map $\psi : G \to U(n)$, defining it by $\psi(\sigma) = k$.

   If $\sigma'(\zeta) = \zeta^{k'}$, we have $(\sigma\circ\sigma')(\zeta) = \sigma(\zeta^{k'}) = \zeta^{kk'}$, so that $\psi(\sigma\circ\sigma') = \psi(\sigma)\cdot\psi(\sigma')$, which proves that ψ is a group homomorphism.

   Now, ψ is injective, because if $\psi(\sigma) = 1$ then $\sigma = id$. Furthermore, we have
   $$|G| = [\mathbb{Q}[\zeta]:\mathbb{Q}] = \varphi(n) = |U(n)|,$$
   so ψ is an isomorphism. ◇

COMMENTARY. – One of the most beautiful theorems of Galois theory, the Kronecker–Weber theorem, states that every normal extension N of finite degree of $\mathbb{Q}$ whose Galois group is abelian (such extensions are called *abelian extensions*, cf. §10.1), is contained in a cyclotomic extension, i.e. an extension generated by a root of unity ζ. In Exercise 9.9, we study a particular case of this theorem, namely, the case of quadratic extensions. The reader can find a proof of the general theorem in the last chapters of the book by Paulo Ribenboim listed in the bibliography. The study of the abelian extensions of $\mathbb{Q}$ is the object of what is known as *class field theory.*

Exercises for Chapter 9

Exercise 9.1. Roots of unity

1) Complex numbers: are the following numbers roots of unity in $\mathbb{C}$?

a) $\dfrac{3\sqrt{6}+7i\sqrt{5}}{17}$

b) $\dfrac{7+4i\sqrt{2}}{9}$

c) $\dfrac{\sqrt{2+\sqrt{3}}+i\sqrt{2-\sqrt{3}}}{2}$

2) Let n be an integer, and let ζ be a primitive n-th root of unity. Let K be an intermediate field between $\mathbb{Q}$ and $\mathbb{Q}[\zeta]$. Show that K is a normal extension of $\mathbb{Q}$.

3) Let m and n be two relatively prime integers. Let ζ be a primitive m-th root of unity and η a primitive n-th root of unity. Show that $\mathbb{Q}[\zeta] \cap \mathbb{Q}[\eta] = \mathbb{Q}$.

4) Let K be a field contained in $\mathbb{C}$, $n \geq 2$ an integer and ζ a primitive n-th root of unity in $\mathbb{C}$. Show that $\mathrm{Gal}(K[\zeta]|K)$ is isomorphic to a subgroup of $U(n)$.

Exercise 9.2. Algebraic numbers of modulus 1 that are not roots of unity

Set $P(X) = (X^2+X+1)^2 - 2X^2$, and let t and u denote the real roots of P, and v and w the non-real roots of P.

1) Show that P is irreducible over $\mathbb{Q}$.

2) Show that v and w are algebraic over $\mathbb{Q}$ and of modulus 1, whereas t and u are algebraic over $\mathbb{Q}$ but not of modulus 1.

3) Deduce that v and w are not roots of unity.

Exercise 9.3. The Möbius function

1) Check, by computing the terms, that $\sum_{d \in D(360)} \mu(d) = 0$.

2) **a)** Show that $n = \sum_{d \in D(n)} \varphi(d)$.

b) Deduce that $\varphi(n) = \sum_{d \in D(n)} d\mu\left(\frac{n}{d}\right)$.

Exercise 9.4. Computation of cyclotomic polynomials

1) For each $n \leq 12$, decompose the polynomial $X^n - 1$ as a product of irreducible factors in $\mathbb{Z}[X]$ and in $\mathbb{Q}[X]$.

2) Using the formula of Proposition 9.4.2 2), determine the cyclotomic polynomials $\Phi_n(X)$ for $n = 30$, $n = 81$.

3) In this question, we propose a rapid way of computing $\Phi_n(X)$ for $n > 1$.

a) Show that $\Phi_n(X) = X^{\varphi(n)}\Phi_n(1/X)$. Deduce that the coefficients of Φ_n satisfy $a_{\varphi(n)-k} = a_k$ for $0 \leq k \leq \varphi(n)$.

b) Show that $\Phi_n(X)$ is determined by its value modulo $X^{[\varphi(n)/2]+1}$, where the square brackets indicate the integral part, and that this computation can be done in the ring $A = \mathbb{Z}[X]/(X^{[\varphi(n)/2]+1})$.

4) Prove the formulas:

$\Phi_n(X) = \Phi_m(X^{n/m})$ whenever m is the product of the distinct prime factors dividing n;

$\Phi_{pn}(X) = \Phi_n(X^p)/\Phi_n(X)$ whenever p is a prime not dividing n;

$\Phi_{2n}(X) = \Phi_n(-X)$ whenever n is an odd integer > 1.

5) Now, use these results to compute the polynomials $\Phi_n(X)$ for $n = 30$, 81, 105.

Exercise 9.5. Fifth roots of unity

Set $\zeta = e^{2i\pi/5}$.

1) Solve the equation $x^4 + x^3 + x^2 + x + 1 = 0$ by using the change of variables $y = x + (1/x)$. Deduce algebraic expressions for ζ^k, $1 \leq k \leq 4$.

2) Without using the results of Chapter 9, define an isomorphism of the group $G = \mathrm{Gal}(\mathbb{Q}[\zeta]|\mathbb{Q})$ onto a well-known group. Show that G has a non-trivial subgroup H of order 2 and index 2.

3) Find an element generating the field $I(H)$, which (we recall) is the set of elements in $\mathbb{Q}[\zeta]$ invariant under H.

Exercise 9.6. Fifteenth roots of unity

Set $\zeta = e^{2i\pi/15}$ and $\eta = e^{2i\pi/5}$, $j = e^{2i\pi/3}$. Recall that

$$\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}.$$

1) What is the degree of $\mathbb{Q}[\zeta]$ over $\mathbb{Q}$?

   Compute the minimal polynomial Φ of ζ over $\mathbb{Q}$.

   Give the decomposition of $X^{15} - 1$ as a product of irreducible factors in $\mathbb{Q}[X]$.

   Set $G = \mathrm{Gal}(\mathbb{Q}[\zeta]|\mathbb{Q})$, and let σ_k denote the element of the group G such that $\sigma_k(\zeta) = \zeta^k$ with $1 \leq k \leq 14$.

2) What are the possible values for k?

3) a) Show that the Galois group G is isomorphic to a product P of two cyclic groups, and construct this isomorphism.

   b) What are the orders of the elements of P?

4) a) Show that $\mathbb{Q}[\sqrt{5}] \subset \mathbb{Q}[\eta]$.

   b) Show that $\mathbb{Q}[\zeta]$ is an extension of degree 2 of $\mathbb{Q}\left[\cos(2\pi/15)\right]$.

5) a) Show that $\mathbb{Q}[j]$, $\mathbb{Q}[\eta]$, $\mathbb{Q}\left[\sqrt{5}\right]$, $\mathbb{Q}\left[j, \sqrt{5}\right]$ are extensions of $\mathbb{Q}$ contained in $\mathbb{Q}[\zeta]$.

   b) For each of the four fields K listed above, determine the subgroup $\mathrm{Gal}(\mathbb{Q}[\zeta]|K)$ of G (give the elements σ_k of each of these groups).

6) **a)** Determine the field of invariants of the subgroup of G generated by σ_{14}.

b) Solve the same problem for the subgroup of G generated by σ_2 (show first that the desired field is a subfield of $\mathbb{Q}\left[j, \sqrt{5}\right]$).

7) Give the trellis of subgroups of P and the trellis of extensions of $\mathbb{Q}$ contained in $\mathbb{Q}[\zeta]$, by making the Galois correspondence completely explicit.

8) Compute an algebraic expression for $\cos(2\pi/15)$ by using the group

$$\mathrm{Gal}\left(\mathbb{Q}\left[\cos\frac{2\pi}{15}\right] | \mathbb{Q}\left[\sqrt{5}\right]\right).$$

9) Using the problems above, decide if the regular polygon with 15 sides (and radius 1) is constructible with ruler and compass.

Exercise 9.7. Seventeenth roots of unity

Set $\zeta = e^{2i\pi/17}$ and $G = \mathrm{Gal}(\mathbb{Q}[\zeta]|\mathbb{Q})$. Let σ_i be the $\mathbb{Q}$-automorphism of $\mathbb{Q}[\zeta]$ defined by $\sigma_k(\zeta) = \zeta^k$ for $k = 1, \ldots, 16$. Note that in this exercise, as in the preceding one, the procedure we use is not entirely algebraic: it is necessary to consider orders of elements to distinguish the roots.

1) Find the smallest integer n such that the class of n modulo 17 generates $(\mathbb{Z}/17\mathbb{Z})^*$. Use this to determine an isomorphism from G to the group $(\mathbb{Z}/16\mathbb{Z}, +)$, and then the trellis of subgroups of G.

2) For every intermediate extension K between $\mathbb{Q}[\zeta]$ and $\mathbb{Q}$, give an element σ_k of G such that $K = I(\langle\sigma_k\rangle)$, the set of elements invariant under $\langle\sigma_k\rangle$.

3) In terms of ζ, determine an x such that $\mathbb{Q}[x]$ is a quadratic extension of degree 2 of $\mathbb{Q}$ contained in $\mathbb{Q}[\zeta]$. Find the minimal polynomial of x over $\mathbb{Q}$. Deduce the value of x.

4) In terms of ζ, determine y such that $\mathbb{Q}[x, y]$ is an extension of degree 2 of $\mathbb{Q}[x]$ contained in $\mathbb{Q}[\zeta]$. Find the minimal polynomial of y over $\mathbb{Q}[x]$, and use it to deduce the value of y.

5) In terms of ζ, determine z such that $\mathbb{Q}[x, y, z]$ is a quadratic extension of $\mathbb{Q}[x, y]$ contained in $\mathbb{Q}[\zeta]$. Find the minimal polynomial of z over $\mathbb{Q}[x, y]$, and use it to deduce the value of z and of $\cos(2\pi/17)$.

6) Deduce the value ζ from the previous computations.

7) Is the regular polygon of radius 1 with 17 sides constructible with ruler and compass?

Exercise 9.8. The structure of $U(n)$

Let n be an integer > 1.

1) **a)** Suppose that p is a prime. What is the structure of $U(p)$?

b) Suppose $n = rs$ with r and s relatively prime. Show that we have $U(n) \simeq U(r) \times U(s)$ and $\varphi(n) = \varphi(r)\varphi(s)$.

c) Determine the structure of $U(n)$ for $n = 2, 4, 6, 8, 9, 12, 15$.

2) Assume that n is of the form p^k, where p is an odd prime and k is an integer > 1.

a) Let a be an integer whose class modulo p generates $(\mathbb{Z}/p\mathbb{Z})^*$. Set $b = a^{p^{k-1}}$. Show that the class of b modulo p^k is of order $p-1$ in $U(n)$.

b) Show that for every $r \geq 0$, we have $(1+p)^{p^r} = 1+p^{r+1} \bmod p^{r+2}$.

c) Deduce that $1+p$ is of order p^{k-1} in $U(n)$, and then that $U(n)$ is cyclic.

d) Determine a generator of $U(25)$, and a generator of $U(125)$.

3) Assume that n is of the form 2^k.

a) Show that for every $r \geq 0$, we have $5^{2^r} = 1 + 2^{r+2} \bmod 2^{r+3}$.

b) Deduce that the class of 5 is of order 2^{k-2} in $U(n)$.

c) Show that, for $k \geq 2$, a power of 5 is never equal to -1 modulo n.

d) Deduce that for every $k \geq 2$, $U(n)$ is isomorphic to $\mathbb{Z}/2^{k-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

e) Determine the order of 3 in $U(n)$.

4) **a)** What is the structure of $U(200)$?

b) Show that the group $U(n)$ is cyclic if and only if n is of the form p^k or $2p^k$, where p is an odd prime (decompose n as a product of prime factors).

Exercise 9.9. Quadratic and cyclotomic extensions

For every integer $n \geq 2$, set $\zeta_n = e^{2i\pi/n}$. We propose to prove the following proposition: for every prime p in $\mathbb{N}$, there exists n in $\mathbb{N}$ such that $\sqrt{p} \in \mathbb{Q}[\zeta_n]$.

1) Show the result for $p = 2$ (take $n = 8$).

From now on, we assume that $p > 2$. Set $P(X) = X^p - 1$, $S(X) = P(X)/(X-1)$, and $\zeta = \zeta_p$.

2) Show that the discriminant $D(S)$ is the square of an element d of $\mathbb{Q}[\zeta]$, and that $D(S)$ is rational.

3) **a)** Show that $S'(x) = (px^{p-1})/(x-1)$ for every root x of S.

b) Deduce that $D(S) = (-1)^{(p-1)/2}p^{p-2}$.

4) **a)** Deduce from the two preceding questions that $\sqrt{p}/d$ or $\sqrt{p}/id$ is rational, by arguing according to the values of p modulo 4.

b) Show that $\mathbb{Q}[i, \zeta_n] = \mathbb{Q}[\zeta_{4n}]$ for every odd integer n.

c) Prove the proposition.

5) Show that for every $N \in \mathbb{Z}$, there exists an integer n such that $\sqrt{N} \in \mathbb{Q}[\zeta_n]$.

Exercise 9.10. Factorization of Φ_p over a quadratic extension of $\mathbb{Q}$

This exercise uses the results of Exercise 9.9.

Let p be an odd prime. Set $\zeta = e^{2i\pi/p}$, $N = \mathbb{Q}[\zeta]$, and $G = \mathrm{Gal}(N|\mathbb{Q}) \simeq U(p)$. Let $\Phi_p(X)$ denote the minimal polynomial of ζ over $\mathbb{Q}$, and let σ_k be the element of G defined by $\sigma_k(\zeta) = \zeta^k$. Let a be a generator of $U(p)$.

Let L denote either the field $\mathbb{Q}\left[\sqrt{p}\right]$ if $p = 1 \bmod 4$ or the field $\mathbb{Q}\left[i\sqrt{p}\right]$ if $p = 3 \bmod 4$.

Recall that for every divisor d of n, a cyclic group of order n has a unique subgroup of order d.

1) Show that $L \subset N$.

2) What is the set of quadratic extensions of $\mathbb{Q}$ contained in N?

3) What is the order of $G' = \mathrm{Gal}(N|L)$? What are its elements, in terms of a?

4) Using 3), show that Φ_p factors as a product of two irreducible polynomials over $L[X]$. Denote them by S and T; give their roots in N and their constant terms.

5) Compute the expression of S and T in $L[X]$ by using the preceding questions:

a) for $p = 7$,

b) for $p = 13$.

Solutions to Some of the Exercises

Solution to Exercise 9.1.

1) a) The modulus is not 1.

b) The modulus is 1, but the minimal polynomial over $\mathbb{Q}$ is $X^2 - (14/9)X + 1$. As it does not have integral coefficients, the number we are considering cannot be a root of unity in $\mathbb{C}$, since the minimal polynomials of roots of unity are the cyclotomic polynomials, and we know that they have integral coefficients.

c) The square of the number is $e^{i\pi/6}$, and its real part is strictly positive, so it must be $e^{i\pi/12}$.

2) $\mathbb{Q}[\zeta]$ is a normal extension of $\mathbb{Q}$ with Galois group $U(n)$. K is the field of invariants of a subgroup H of $U(n)$. As $U(n)$ is abelian, H is a normal subgroup of it, so K is a normal extension of $\mathbb{Q}$.

3) Let ω be a primitive mn-th root of unity. The degree of $\mathbb{Q}[\omega]$ over $\mathbb{Q}$ is $\varphi(mn) = \varphi(m)\varphi(n)$ (this equality holds because m and n are relatively prime).

As $\mathbb{Q}[\zeta]$ is of degree $\varphi(m)$ over $\mathbb{Q}$, and $\mathbb{Q}[\eta]$ is of degree $\varphi(n)$ over $\mathbb{Q}$, the tower rule shows that $\mathbb{Q}[\omega]$ is of degree $\varphi(m)$ over $\mathbb{Q}[\eta]$ and $\varphi(n)$ over $\mathbb{Q}[\zeta]$. Set $L = \mathbb{Q}[\zeta] \cap \mathbb{Q}[\eta]$, $r = [\mathbb{Q}[\zeta] : L]$. As L is an intermediate extension between $\mathbb{Q}$ and $\mathbb{Q}[\zeta]$, we have $r \leq \varphi(m)$ (Figure 9.2). Furthermore, the degree of ζ over L is greater than or equal to the degree of ζ over $\mathbb{Q}[\eta]$; as $\mathbb{Q}[\omega] = \mathbb{Q}[\eta][\zeta]$, we have $r \geq \varphi(m)$ and thus the result.

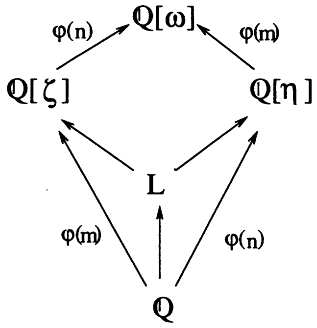


FIGURE 9.2.

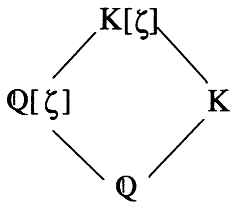


FIGURE 9.3.

We can also use the isomorphism $U(mn) \simeq U(m) \times U(n)$; the intermediate extensions $\mathbb{Q}[\zeta]$ and $\mathbb{Q}[\eta]$ corresponding to the subgroups $U(m) \times \{\text{id}\}$ and $\{\text{id}\} \times U(n)$ of $U(m) \times U(n)$ have intersection equal to $\mathbb{Q}$ (see Exercise 8.6).

4) Because $K[\zeta]$ is the splitting field of $X^n - 1$ over K (Figure 9.3), it is a normal extension of K. As $K[\zeta] \supset \mathbb{Q}[\zeta]$ and $\mathbb{Q}[\zeta]$ is a normal extension of $\mathbb{Q}$, every element of $\text{Gal}(K[\zeta]|K)$ induces an element of $\text{Gal}(\mathbb{Q}[\zeta]|\mathbb{Q}) \simeq U(n)$ by restriction. This restriction is a group homorphism, which is injective because if $\sigma \in \text{Gal}(K[\zeta]|K)$ induces the identiy on $\mathbb{Q}[\zeta]$, then $\sigma(\zeta) = \zeta$, so $\sigma = \text{id}$.

Solution to Exercise 9.2.

1) In the field $\mathbb{Q}\left[\sqrt{2}\right][X]$, we have

$$P(X) = \left(X^2 + (1 - \sqrt{2})X + 1\right)\left(X^2 + (1 + \sqrt{2})X + 1\right).$$

The roots of P are given by

$$\begin{aligned} t, u &= \frac{-1 - \sqrt{2} \pm \sqrt{2\sqrt{2} - 1}}{2} \\ v, w &= \frac{\sqrt{2} - 1 \pm i\sqrt{2\sqrt{2} + 1}}{2}. \end{aligned}$$

Note first that P has no linear factor in $\mathbb{Q}[X]$. Next, note that a decomposition into two quadratic factors is impossible in $\mathbb{Q}[X]$, since one of the factors must be $X^2 + (1 + \sqrt{2})X + 1$.

2) The computations are not difficult.

3) The conjugates of roots of unity over $\mathbb{Q}$ are also roots of unity; as t and u do not have modulus 1, their conjugates v and w over $\mathbb{Q}$ are not roots of unity.

Solution to Exercise 9.3.

1) $\mu(d)$ is not zero when d is squarefree, so we have

$$\sum_{d\in D(360)} \mu(d) = \mu(1)+\mu(2)+\mu(3)+\mu(5)+\mu(6)+\mu(10)+\mu(15)+\mu(30)$$
$$= 1-1-1-1+1+1+1-1 = 0.$$

2) a) In $\mathbb{Z}/n\mathbb{Z}$, we know that the order of every element divides n. For a divisor d of n, let E_d denote the set of elements of order d. The family $(E_d)_{d\in D(n)}$ is a partition of $\mathbb{Z}/n\mathbb{Z}$, and we know that E_d has $\varphi(d)$ elements. This gives the result.

b) To obtain the results, it suffices to apply the Möbius inversion formula with $f = \text{id}$ and $g = \varphi$.

Solution to Exercise 9.4.

1) We can use the formula $X^n - 1 = \prod_{d\in D(n)} \Phi_d(X)$, or simply make a direct computation. Up to invertible factors, the decompositions are the same in $\mathbb{Z}[X]$ and in $\mathbb{Q}[X]$:

$$\begin{aligned}
X^2-1 &= (X-1)(X+1),\\
X^3-1 &= (X-1)(X^2+X+1),\\
X^4-1 &= (X-1)(X+1)(X^2+1),\\
X^5-1 &= (X-1)\Phi_5(X),\\
X^6-1 &= (X-1)(X^2+X+1)(X+1)(X^2-X+1),\\
X^7-1 &= (X-1)\Phi_7(X),\\
X^8-1 &= (X-1)(X+1)(X^2+1)(X^4+1),\\
X^9-1 &= (X^3-1)(X^6+X^3+1),\\
X^{10}-1 &= (X-1)\Phi_5(X)(X+1)\Phi_5(-X),\\
X^{11}-1 &= (X-1)\Phi_{11}(X),\\
X^{12}-1 &= (X^6-1)(X^2+1)(X^4-X^2+1),\\
&= (X-1)(X^2+X+1)(X+1)\cdot\\
&\quad (X^2-X+1)(X^2+1)(X^4-X^2+1)
\end{aligned}$$

2) We have

$$\begin{aligned}
[t]\Phi_{30}(X) &= \frac{(X^{30}-1)(X^5-1)(X^3-1)(X^2-1)}{(X^{15}-1)(X^{10}-1)(X^6-1)(X-1)}\\
&= \frac{(X^{15}+1)(X+1)}{(X^5+1)(X^3+1)}
\end{aligned}$$

$$\begin{aligned} &= \frac{X^{10}-X^5+1}{X^2-X+1} \\ &= X^8+X^7-X^5-X^4-X^3+X+1, \\ \Phi_{81}(X) &= \frac{X^{81}-1}{X^{27}-1} \\ &= X^{54}+X^{27}+1. \end{aligned}$$

3) a) Set $S = \sum_{d\in D(n)} \mu(n/d)$. We know that $S = 0$ for $n > 1$. Furthermore, by the preceding exercise, $\varphi(n) = \sum_{d\in D(n)} d\mu(n/d)$. Consequently, we have

$$\begin{aligned} X^{\varphi(n)}\Phi_n\left(\frac{1}{X}\right) &= X^{\varphi(n)} \prod_{d\in D(n)} (X^{-d}-1)^{\mu(n/d)} \\ &= (-1)^S \prod_{d\in D(n)} (X^d-1)^{\mu(n/d)} \\ &= \Phi_n(X). \end{aligned}$$

If $\Phi_n(X) = \sum_{0\le k\le\varphi(n)} a_kX^k$, the preceding equality shows that $a_k = a_{\varphi(n)-k}$.

b) It suffices to compute the terms of $\Phi_n(X)$ of degree $\le \frac{\varphi(n)}{2}$. The polynomials of the form 1 - X^k are invertible in A, since the X^k are nilpotent.

4) We have

$$\begin{aligned} \Phi_n(X) &= \prod_{d\in D(n)} (X^{n/d}-1)^{\mu(d)} \\ &= \prod_{d\in D(m)} ((X^{n/m})^{m/d}-1)^{\mu(d)} \\ &= \Phi_m(X^{n/m}), \\ \Phi_{pn}(X) &= \prod_{d\in D(n)} (X^{pn/d}-1)^{\mu(d)} \prod_{d\in D(pn)-D(n)} (X^{pn/d}-1)^{\mu(d)} \\ &= \prod_{d\in D(n)} ((X^p)^{n/d}-1)^{\mu(d)} \prod_{d\in D(n)} ((X^{n/d}-1)^{-\mu(d)} \\ &= \frac{\Phi_n(X^p)}{\Phi_n(X)}, \\ \Phi_{2n}(X) &= \frac{\Phi_n(X^2)}{\Phi_n(X)} \end{aligned}$$

$$\begin{aligned}
&= \prod_{d\in D(n)} (X^{2n/d}-1)^{\mu(d)}(X^{n/d}-1)^{-\mu(d)} \\
&= \prod_{d\in D(n)} (X^{n/d}+1)^{\mu(d)} \\
&= (-1)\sum_{d\in D(n)}\mu(d) \prod_{d\in D(n)} (X^{n/d}-1)^{\mu(d)} \\
&= \Phi_n(-X),
\end{aligned}$$

since n/d is odd and $\sum_{d\in D(n)} \mu(d) = 0$ for $n > 1$.

5) To compute Φ_{30}, we can reason modulo X^5, since $\varphi(30) = 8$. Modulo X^5, we have

$$\begin{aligned}
\Phi_{30}(X) &= \frac{(X^{30}-1)(X^5-1)(X^3-1)(X^2-1)}{(X^{15}-1)(X^{10}-1)(X^6-1)(X-1)} \\
&= \frac{(-1)(-1)(X^3-1)(X^2-1)}{(-1)(-1)(-1)(X-1)} \\
&= -(X^3-1)(X+1) \\
&= -X^4-X^3+X+1,
\end{aligned}$$

which gives the result.

To compute Φ_{81}, we can write $\Phi_{81}(X) = \Phi_3(X^{27})$. Because $\varphi(81)/2 = 27$, we can compute modulo X^{28} : $\Phi_{81}(X) = (X^{81}-1)/(X^{27}-1) = X^{27}+1$, etc.

To compute Φ_{105}, we compute modulo X^{25} since $\varphi(105) = 48$. Modulo X^{25}, we have

$$\begin{aligned}
\Phi_{105}(X) &= \frac{(X^{105}-1)(X^5-1)(X^3-1)(X^7-1)}{(X^{15}-1)(X^{21}-1)(X^{35}-1)(X-1)} \\
&= (X^5-1)(X^2+X+1)(X^7-1)(1+X^{15})(1+X^{21}) \\
&= -X^{24}-X^{22}-X^{20}+X^{17}+X^{16}+X^{15}+X^{14}+X^{13}+ \\
&\qquad X^{12}-X^9-X^8-2X^7-X^6-X^5+X^2+X+1,
\end{aligned}$$

so

$$\begin{aligned}
\Phi_{105}(X) &= X^{48}+X^{47}+X^{46}-X^{45}-X^{44}-2X^{43}-X^{42}-X^{41}+ \\
&\quad X^{38}+X^{37}+X^{36}+X^{35}+X^{34}+X^{33}-X^{30}- \\
&\quad X^{28}-X^{26}-X^{24}-X^{22}-X^{20}+X^{17}+X^{16}+ \\
&\quad X^{15}+X^{14}+X^{13}+X^{12}-X^9-X^8-2X^7- \\
&\quad -X^6-X^5+X^2+X+1.
\end{aligned}$$

It so happens that the coefficients of Φ_n with $n < 105$ all lie in the set $\{-1,0,1\}$; however, this result shows that this is not always the case.

Solution to Exercise 9.5.

1) The equation becomes y^2+y-1, so we have $y = (-1 \pm \sqrt{5})/2$. For the two values y, the equations $x^2 - xy + 1 = 0$ give

$$x = \frac{-1+\sqrt{5}}{4} \pm i\frac{\sqrt{10+2\sqrt{5}}}{4} \quad \text{or} \quad \frac{-1-\sqrt{5}}{4} \pm i\frac{\sqrt{10-2\sqrt{5}}}{4}.$$

We need an additional argument, using the ordering on $\mathbb{R}$, to be able to deduce the values of the ζ^k for $1 \le k \le 4$ from these four numbers.

For this, we consider the values of the real parts $2\cos(2\pi/5) = (-1+\sqrt{5})/2$ and $2\cos(4\pi/5) = (-1-\sqrt{5})/2$ and the values of the imaginary parts. We find that

$$\begin{aligned}
\zeta &= \frac{-1+\sqrt{5}}{4} + i\frac{\sqrt{10+2\sqrt{5}}}{4},\\
\zeta^2 &= \frac{-1-\sqrt{5}}{4} + i\frac{\sqrt{10-2\sqrt{5}}}{4},\\
\zeta^3 &= \frac{-1-\sqrt{5}}{4} - i\frac{\sqrt{10-2\sqrt{5}}}{4},\\
\zeta^4 &= \frac{-1+\sqrt{5}}{4} - i\frac{\sqrt{10+2\sqrt{5}}}{4}.
\end{aligned}$$

2) As $[\mathbb{Q}[\zeta]:\mathbb{Q}] = 4$, G has four elements. They are determined by the image of ζ. Let σ denote the $\mathbb{Q}$-homorphism defined by $\sigma(\zeta) = \zeta^2$. As $\sigma^2(\zeta) = \zeta^4$, $\sigma^3(\zeta) = \zeta^3$, and $\sigma^4(\zeta) = \zeta$, we have $\sigma^4 = \mathrm{id}$, σ is of order 4 in G, and G is isomorphic to $\mathbb{Z}/4\mathbb{Z}$. This last group has only one non-trivial subgroup, generated by the class of 2, which corresponds to the subgroup H of G generated by σ^2.

3) As $\sqrt{5} = 2(\zeta+\zeta^4)+1$, we see that $\mathbb{Q}[\sqrt{5}]$ must be the extension corresponding to H.

Solution to Exercise 9.6.

1) We know that $[\mathbb{Q}[\zeta]:\mathbb{Q}] = \varphi(15)$, where φ denotes the Euler function. As $\varphi(15) = \varphi(3)\varphi(5) = 8, \mathbb{Q}[\zeta]$ is an extension of degree 8 of $\mathbb{Q}$.

The minimal polynomial Φ of ζ over $\mathbb{Q}$ is the cyclotomic polynomial $\Phi_{15}(X)$. The formulas of Proposition 9.4.2 give

$$\Phi_{15}(X) = \frac{(X^{15}-1)(X-1)}{(X^5-1)(X^3-1)}$$

$$\begin{aligned} &= X^8 - X^7 + X^5 - X^4 + X^3 - X + 1, \\ X^{15} - 1 &= \Phi_{15}(X)\Phi_5(X)\Phi_3(X)\Phi_1(X) \\ &= (X^8 - X^7 + X^5 - X^4 + X^3 - X + 1) \cdot \\ &\qquad (X^4 + X^3 + X^2 + X + 1)(X^2 + X + 1)(X - 1). \end{aligned}$$

2) The image ζ^k of ζ under σ_k is a primitive 15th root of unity, so k is prime to 15 ; thus, the possible values of k are the eight numbers 1, 2, 4, 7, 8, 11, 13, and 14.

3) a) We know that G is isomorphic to the group $U(15)$ of invertible elements of the ring $\mathbb{Z}/15\mathbb{Z}$. This last group is isomorphic to $U(3) \times U(5)$, so to $P = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. The isomorphism is thus the composition

$$G \xrightarrow{\varphi} U(15) = (\mathbb{Z}/15\mathbb{Z})^* \xrightarrow{\chi} (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^* \xrightarrow{\psi} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z},$$

where $\varphi(\sigma) = k$ such that $\sigma(\zeta) = \zeta^k$, $\chi(k) = (k \bmod 3, k \bmod 5)$ and ψ is the isomorphism defined by choosing the classes of 2 modulo 3 and modulo 5 as generators of $(\mathbb{Z}/3\mathbb{Z})^*$ and $(\mathbb{Z}/5\mathbb{Z})^*$. This is made explicit in Table 9.1.

σ	σ_1	σ_2	σ_4	σ_7	σ_8	σ_{11}	σ_{13}	σ_{14}
$\varphi(\sigma)$	1	2	4	7	8	11	13	14
$\chi(\varphi(\sigma))$	(1,1)	(2,2)	(1,4)	(1,2)	(2,3)	(2,1)	(1,3)	(2,4)
$\psi(\chi(\varphi(\sigma)))$	(0,0)	(1,1)	(0,2)	(0,1)	(1,3)	(1,0)	(0,3)	(1,2)

TABLE 9.1.

b) Here, we let 2 and 4 denote the classes modulo 2 and 4; P has three elements of order two, namely $(0,2)$, $(1,0)$, $(1,2)$, and four elements of order 4, namely $(0,1)$, $(1,1)$, $(0,3)$ $(1,3)$.

4) a) As $\cos(2\pi/5) = (-1+\sqrt{5})/4 = (\eta + \eta^{-1})/2$, we have $\mathbb{Q}[\sqrt{5}] \subset \mathbb{Q}[\eta]$.

b) As $2\cos(2\pi/15) = \zeta + \zeta^{-1}$, we see that $\mathbb{Q}[\cos(2\pi/15)] \subset \mathbb{Q}[\zeta]$. This inclusion is strict since ζ is not real; as $\zeta^2 - 2\zeta\cos(2\pi/15) + 1 = 0$, $\mathbb{Q}[\zeta]$ is a quadratic extension of $\mathbb{Q}[\cos(2\pi/15)]$.

5) a) As $j = \zeta^5$ and $\eta = \zeta^3$, $\mathbb{Q}[j]$ and $\mathbb{Q}[\eta]$ are extensions of $\mathbb{Q}$ contained in $\mathbb{Q}[\zeta]$. We know that $\mathbb{Q}[\cos(2\pi/5)] \subset \mathbb{Q}[\eta]$, which shows that $\mathbb{Q}[\sqrt{5}]$ is contained in $\mathbb{Q}[\zeta]$. The preceding inclusions show that $\mathbb{Q}[j, \sqrt{5}] \subset \mathbb{Q}[\zeta]$.

b) $K = \mathbb{Q}[j]$. We have $\sigma_k \in \mathrm{Gal}(\mathbb{Q}[\zeta]|\mathbb{Q}[j])$ if and only if $\sigma_k(j) = j$; as $j = \zeta^5$, this means that $5k = 5 \bmod 15$ or $k = 1 \bmod 3$, so $k = 1, 4, 7, 13$. The Galois group is cyclic, generated by σ_7.

$K = \mathbb{Q}[\eta]$. We have $\sigma_k \in \mathrm{Gal}(\mathbb{Q}[\zeta]|\mathbb{Q}[\eta])$ if and only if $\sigma_k(\eta) = \eta$. As $\eta = \zeta^3$, this means that $3k = 3 \bmod 15$ or $k = 1 \bmod 5$, so $k = 1, 11$.

$K = \mathbb{Q}[\sqrt{5}]$. As $\mathbb{Q}[\sqrt{5}] = \mathbb{Q}[\eta + \eta^{-1}]$, $\sigma_k \in \text{Gal}\left(\mathbb{Q}[\zeta]|\mathbb{Q}[\sqrt{5}]\right)$ if and only if $\sigma_k(\eta + \eta^{-1}) = \eta + \eta^{-1}$. This means that

$$\cos k\frac{2\pi}{5} = \cos\frac{2\pi}{5}, \qquad \text{i.e.} \qquad k = \pm 1 \bmod 5,$$

so $k = 1, 4, 11, 14$. The Galois group is not cyclic; it has three elements of order 2.

$K = \mathbb{Q}[j, \sqrt{5}]$. As $\text{Gal}\left(\mathbb{Q}[\zeta]|\mathbb{Q}[j, \sqrt{5}]\right)$ is the intersection of the two groups $\text{Gal}(\mathbb{Q}[\zeta]|\mathbb{Q}[j])$ and $\text{Gal}(\mathbb{Q}[\zeta]|\mathbb{Q}[\sqrt{5}]$, it contains σ_k for $k = 1, 4$.

At this stage of the problem, we can begin to construct the trellises.

6) a) Set $K = I(\langle\sigma_{14}\rangle)$. As σ_{14} is of order 2, $\mathbb{Q}[\zeta]$ is a quadratic extension of K. We see that $\cos(2\pi/15) = (\zeta + \zeta^{-1})/2$ is invariant under σ_{14}, so we have $\mathbb{Q}[\cos(2\pi/15)] \subset K$. Then, by 4 **b)** of this exercise, we can conclude that $K = \mathbb{Q}[\cos(2\pi/15)]$.

b) Set $L = I(\langle\sigma_2\rangle)$. As σ_2 is of order 4, $\mathbb{Q}[\zeta]$ is an extension of degree 4 of L, so L is an extension of degree 2 of $\mathbb{Q}$. As $(\sigma_2)^2 = \sigma_4$, L is a subfield of $I(\langle\sigma_4\rangle) = \mathbb{Q}[j, \sqrt{5}]$. Note that $\sqrt{5}$ does not lie in L, since σ_2 is not in the group $\text{Gal}\left(\mathbb{Q}[\zeta]|\mathbb{Q}[\sqrt{5}]\right)$. Thus, by the preceding question, we have $\sigma_2(\sqrt{5}) = -\sqrt{5}$; furthermore, $\sigma_2(j) = j^2 = -1 - j$. It follows that those elements $a + bj + c\sqrt{5} + dj\sqrt{5}$ of $\mathbb{Q}[j, \sqrt{5}]$ which are invariant under σ_2 are of the form $a + c\sqrt{5}(1 + 2j)$, i.e. $a + ci\sqrt{15}$. This gives $L = \mathbb{Q}[i\sqrt{15}]$.

7) The trellis of subgroups of P contains three subgroups with two elements, generated by the elements of order 2 of P, and three subgroups with four elements: two generated by elements of order 4 of P (each containing two elements of order 4 and the element $(0, 2)$) and the last one containing the three elements of order 2 of P, isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Questions 5 and 6 contained several hints for the construction of the trellis corresponding to the extensions of $\mathbb{Q}$ contained in $\mathbb{Q}[\zeta]$ (Figure 9.4).

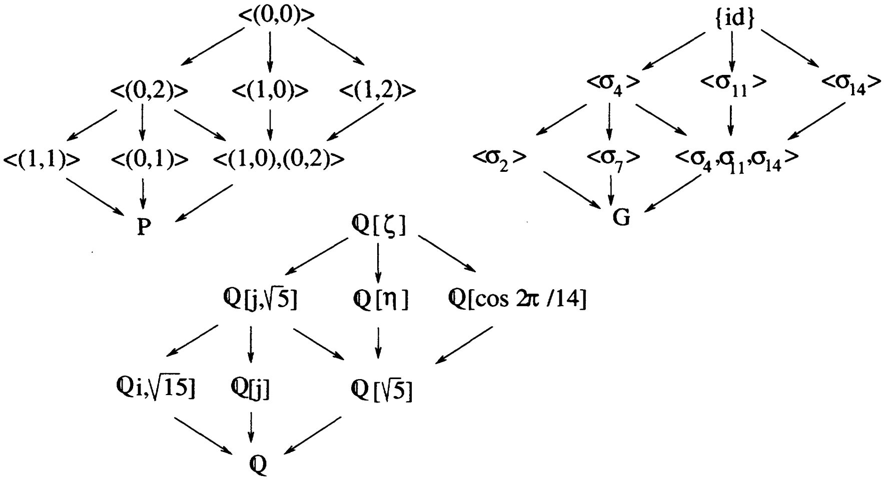


FIGURE 9.4. The Galois correspondence

8) The Galois group $\mathrm{Gal}\big(\mathbb{Q}[\cos(2\pi/15)] \mid \mathbb{Q}[\sqrt{5}]\big)$ is of order 2, generated by the restriction of σ_4. Thus, $\cos(2\pi/15)$ is a root of the polynomial

$$X^2 - \left[\cos\frac{2\pi}{15} + \sigma_4\left(\cos\frac{2\pi}{15}\right)\right] X + \cos\frac{2\pi}{15}\sigma_4\left(\cos\frac{2\pi}{15}\right)$$

whose coefficients lie in $\mathbb{Q}\left[\sqrt{5}\right]$.

Because $\Phi_{15}(\zeta) = 0$ implies that $\zeta^4 - \zeta^3 + \zeta^1 - 1 + \zeta^{-1} - \zeta^{-3} + \zeta^{-4}$, we have

$$\begin{aligned}\cos\frac{2\pi}{15} + \sigma_4\left(\cos\frac{2\pi}{15}\right) &= \frac{\zeta + \zeta^{-1} + \zeta^4 + \zeta^{-4}}{2} \\ &= \frac{\zeta^3 + 1 + \zeta^{-3}}{2} \\ &= \cos\frac{2\pi}{5} + \frac{1}{2} = \frac{1+\sqrt{5}}{4},\end{aligned}$$

$$\begin{aligned}\cos\frac{2\pi}{15}\sigma_4\left(cos\frac{2\pi}{15}\right) &= \frac{(\zeta + \zeta^{-1})(\zeta^4 + \zeta^{-4})}{4} \\ &= \frac{\zeta^3 + \zeta^{-3} + \zeta^5 + \zeta^{-5}}{4} \\ &= \frac{1}{2}\left(\cos\frac{2\pi}{5} + \cos\frac{2\pi}{3}\right) = \frac{-3+\sqrt{5}}{8}.\end{aligned}$$

It follows that $\cos(2\pi/15) = (1+\sqrt{5}+\sqrt{30-6\sqrt{5}})/8$, since $\cos(2\pi/15) > 0$. Thus,

$$\sigma_4\left(\cos\frac{2\pi}{15}\right) = \frac{\zeta^4+\zeta^{-4}}{2} = \cos\frac{8\pi}{15} = \frac{1+\sqrt{5}-\sqrt{30-6\sqrt{5}}}{8}.$$

We could find the same result more rapidly by using

$$\cos(2\pi/15) = \cos\left((\pi/3) - (\pi/5)\right)\dots$$

but that method does not employ the beautiful results of Chapter 9!

9) The regular polygon with 15 sides and radius 1 is constructible with ruler and compass. As in the preceding problem, we can note that the regular polygons with 6 and 10 sides are constructible, and that $(2\pi/15) = (\pi/3) - (\pi/5)$. We can also use Proposition 5.7, and then the preceding problems show that $\mathbb{Q}[\cos(2\pi/15)]$ has an increasing sequence of subfields $\mathbb{Q}$ $\mathbb{Q}[\sqrt{5}]$, $\mathbb{Q}[\cos(2\pi/15)]$, each of degree 2 over the preceding one (this is exactly what is expressed by the formula for $\cos(2\pi/15)$, which only uses extractions of square roots).

Solution to Exercise 9.7.

Recall that $\mathbb{Q}[\zeta]$ is an extension of degree $\varphi(17) = 16$ of $\mathbb{Q}$, which has basis $(\zeta^k)_{1\leq k\leq 16}$ as a $\mathbb{Q}$-vector space.

1) We find $2^8 = 1 \bmod 17$; 3 is of order 16 and works. The isomorphism of $(\mathbb{Z}/16\mathbb{Z},+)$ onto G is the composition

$$\mathbb{Z}/16\mathbb{Z} \xrightarrow{\varphi} U(17) \xrightarrow{\psi} G,$$

with $\varphi(r) = 3^r$ and $\psi(k) = \sigma_k$. It is given in Table 9.2.

0	1	2	3	4	5	6	7
id	σ_3	σ_9	σ_{10}	σ_{13}	σ_5	σ_{15}	σ_{11}

8	9	10	11	12	13	14	15
σ_{16}	σ_{14}	σ_8	σ_7	σ_4	σ_{12}	σ_2	σ_6

TABLE 9.2.

Since the trellis of subgroups of $(\mathbb{Z}/16\mathbb{Z},+)$ is given by

$$\begin{aligned}\{0\} &\subset \langle 8\rangle = (8\mathbb{Z}/16\mathbb{Z},+) \subset \langle 4\rangle = (4\mathbb{Z}/16\mathbb{Z},+)\\ &\subset \langle 2\rangle = (2\mathbb{Z}/16\mathbb{Z},+) \subset (\mathbb{Z}/16\mathbb{Z},+),\end{aligned}$$

and we have $\sigma_9 = (\sigma_3)^2$, $\sigma_{13} = (\sigma_3)^4$, $\sigma_{16} = (\sigma_3)^8$, we find that the trellis of subgroups of G is given by

$$\{\mathrm{id}\} \subset \langle\sigma_{16}\rangle \subset \langle\sigma_{13}\rangle \subset \langle\sigma_9\rangle \subset \langle\sigma_3\rangle = G$$

(we can also note that $\langle\sigma_9\rangle = \langle\sigma_2\rangle, \langle\sigma_{13}\rangle = \langle\sigma_4\rangle$).

2) By the Galois correspondence, we can give the trellis of extensions of $\mathbb{Q}$ contained in $\mathbb{Q}[\zeta]$:

$$I(\{\mathrm{id}\}) = \mathbb{Q}[\zeta] \supset I(\langle\sigma_{16}\rangle) \supset I(\langle\sigma_{13}\rangle) \supset I(\langle\sigma_9\rangle) \supset I(\langle\sigma_3\rangle) = I(G) = \mathbb{Q}.$$

3) As $\langle\sigma_9\rangle$ is a subgroup of index 2 of $\langle\sigma_3\rangle = G$, $I(\langle\sigma_9\rangle)$ is a quadratic extension of $\mathbb{Q}$. The elements of $I(\langle\sigma_9\rangle)$ are the $u \in \mathbb{Q}[\zeta]$ such that $\sigma_9(u) = u$. As u is of the form $\sum_{1\le k\le 16} a_k\zeta^k$, $\sigma_9(u) = u$ implies that the coefficients a_k of index 1, 9, 13, 15, 16, 8, 4, 2 are equal, as well as the coefficients a_k of index 3, 10, 5, 11, 14, 7, 12, 6.

Set $x = \zeta + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2$ (we could have set $x = \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} + \zeta^6$). We have $x \in I(\langle\sigma_9\rangle)$ and $x \notin \mathbb{Q}$ since $\mathbb{Q} = I(\langle\sigma_3\rangle)$ and $\sigma_3(x) \neq x$. Thus, x is of degree 2 over $\mathbb{Q}$ and $I(\langle\sigma_9\rangle) = \mathbb{Q}[x]$. As $\mathrm{Gal}(\mathbb{Q}[x]|\mathbb{Q}) = \langle\sigma_3\rangle/\langle\sigma_9\rangle$ is a group of order 2, the conjugate of x over $\mathbb{Q}$ is $\sigma_3(x)$ since $\sigma_3 \notin \langle\sigma_9\rangle$. The minimal polynomial of x over $\mathbb{Q}$ is $X^2 - (x + \sigma_3(x))X + x\sigma_3(x)$. We see that $x + \sigma_3(x) = \sum_{1\le k\le 16} \zeta^k = -1$, since $\sum_{0\le k\le 16} \zeta^k = 0$. The computation of $x\sigma_3(x)$ is longer: the expansion of the product has 64 terms. After regrouping them, using the equality $\sum_{0\le k\le 16} \zeta^k = 0$, we find $x\sigma_3(x) = -4$; x is a root of the polynomial $X^2 + X - 4$, so $x = (-1 \pm \sqrt{17})/2$. Note that $\mathbb{Q}[x] = \mathbb{Q}[\sqrt{17}]$.

We now need to use an order argument to tell which of these two values is actually x. As $x = 2\cos(2\pi/17) + 2\cos(4\pi/17) + 2\cos(8\pi/17) + 2\cos(16\pi/17)$, we have $x > (0,5 + 0,5 - 1) > 0$, so $x = (-1 + \sqrt{17})/2$, $\sigma_3(x) = (-1 - \sqrt{17})/2$.

4) We use the same procedure as in the preceding question.

The extension $I(\langle\sigma_{13}\rangle)$ is a quadratic extension of degree 2 of $I(\langle\sigma_9\rangle) = \mathbb{Q}[x]$ since $\langle\sigma_{13}\rangle$ is a subgroup of index 2 of $\langle\sigma_9\rangle$. It is generated by any element $y \in I(\langle\sigma_{13}\rangle)$ not in $\mathbb{Q}[x]$.

The search for $u = \sum_{1\le k\le 16} a_k\zeta^k$ satisfying $\sigma_{13}(u) = u$ leads to setting $y = \zeta + \zeta^4 + \zeta^{-4} + \zeta^{-1}$, for example.

We have $y \in I(\langle\sigma_{13}\rangle)$ and $y \notin \mathbb{Q}[x]$ since $\sigma_9(y) \neq y$. Thus, y is of degree 2 over $\mathbb{Q}[x]$ and $I(\langle\sigma_{13}\rangle) = \mathbb{Q}[x, y]$. As $\mathrm{Gal}(\mathbb{Q}[x, y]|\mathbb{Q}[x]) = \langle\sigma_9\rangle/\langle\sigma_{13}\rangle$, the conjugate of y over $\mathbb{Q}[x]$ is $\sigma_9(x)$ since $\sigma_9 \notin \langle\sigma_{13}\rangle$. The minimal polynomial of y over $\mathbb{Q}[x]$ is $X^2 - (y + \sigma_9(y))X + y\sigma_9(y)$.

We see that $y + \sigma_9(y) = x$ and $y\sigma_9(y) = -1$, so y is a root of the polynomial $X^2 - xX - 1$. Thus, $y = (x \pm \sqrt{x^2+4})/2$. We have $\mathbb{Q}[x,y] = \mathbb{Q}[\sqrt{17}, \sqrt{34-2\sqrt{17}}]$ since $x^2+4 = 8 - x = (34 - 2\sqrt{17})/4$.

As $y = \zeta + \zeta^4 + \zeta^{13} + \zeta^{16} = 2\cos(2\pi/17) + 2\cos(8\pi/17) > 0$, we have $y = (x + \sqrt{x^2+4})/2$ and $\sigma_9(y)y = (x - \sqrt{x^2+4})/2$.

5) Still using the same procedure, we determine the extension $I(\langle\sigma_{16}\rangle)$. The search for the $u = \sum_{1\le k\le 16} a_k\zeta^k$ satisfying $\sigma_{16}(u) = u$ leads to setting $z = \zeta + \zeta^{-1}$, for example, checking that $z \notin \mathbb{Q}[x,y]$ since $\sigma_{13}(z) \neq z$. The minimal polynomial of z over $\mathbb{Q}[x,y]$ is $X^2 - (z+\sigma_{13}(z))X + z\sigma_{13}(z)$. We see that $z + \sigma_{13}(z) = y$. Furthermore, $z\sigma_{13}(z) = \zeta^3 + \zeta^5 + \zeta^{12} + \zeta^{14}$ is an element of $\mathbb{Q}[x,y]$, which we need to express in the basis $(1, x, y, xy)$. Computing xy in terms of ζ, we find $xy = 3 + \zeta^2 + \zeta^8 + \zeta^9 + \zeta^{15} + 2(\zeta^3 + \zeta^5 + \zeta^{12} + \zeta^{14})$, so $z\sigma_{13}(z) = (xy - x + y - 3)/2$. Denote this quantity by a; then z is a root of the polynomial $X^2 - yX + a$, so $z = (y \pm \sqrt{y^2 - 4a})/2 = (y \pm \sqrt{2x - 2y - xy + 7})/2$.

As $z = 2\cos(2\pi/17) > \sigma_{13}(z) = 2\cos(8\pi/17)$, we have

$$z = \frac{y + \sqrt{2x - 2y - xy + 7}}{2}, \quad \sigma_{13}(z) = \frac{y - \sqrt{2x - 2y - xy + 7}}{2}.$$

After completing the computations, we obtain

$$\cos\frac{2\pi}{17} = \frac{z}{2} =$$

$$\frac{-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + \sqrt{68 + 12\sqrt{17} - 4\sqrt{34 - 2\sqrt{17}} - 8\sqrt{34 + 2\sqrt{17}}}}{16}.$$

This expression can be found, in varying forms, in the literature. The cosine of the other multiples of $2\pi/17$ are obtained with analogous computations. The formulas that develop are analogues of the preceding ones, up to some sign changes.

6) Finally, $\zeta = \cos(2\pi/17) + i\sin(2\pi/17) = (z + i\sqrt{4 - z^2})/2$.

All of these results are due to Gauss (Figure 9.5).

$$\cos\frac{P}{17} = -\tfrac{1}{16} + \tfrac{1}{16}\sqrt{17} + \tfrac{1}{16}\sqrt{(34-2\sqrt{17})} - \tfrac{1}{8}\sqrt{\{(17+3\sqrt{17}) - \sqrt{(34-2\sqrt{17})} - 2\sqrt{(34+2\sqrt{17})}\}};$$

les cosinus des multiples de cet angle ont une forme semblable, les sinus ont un radical de plus. Il y a certainement bien lieu de s'étonner que la divisibilité du cercle en 3 et 5 parties ayant été connue dès le temps d'*Euclide*, on n'ait rien ajouté à ces découvertes dans un intervalle de deux mille ans, et que tous les géomètres aient annoncé comme certain, qu'excepté ces divisions et celles qui s'en déduisent (les divisions en 2^μ, 15, 3.2^μ, 5.2^μ, 15.2^μ parties), on ne pouvait en effectuer aucune par des constructions géométriques.

FIGURE 9.5. Gauss: *Recherches arithmétiques* (value of $\cos\frac{2\pi}{17}$)

Solution to Exercise 9.9.

1) As $\zeta_8 = \mathrm{e}^{i\pi/4} = (1+i)/\sqrt{2}$, we have $\sqrt{2} = (1+\zeta_8^2)/\zeta_8$ so $\sqrt{2} \in \mathbb{Q}[\zeta_8]$.

2) The roots of S are of the form ζ^i with $1 \le i \le p-1$, so $D(S) = \prod_{1\le i<j\le p-1} (\zeta^i - \zeta^j)^2$ is the square of $d = \prod_{1\le i<j\le p-1} (\zeta^i - \zeta^j)$, which is obviously an element of $\mathbb{Q}[\zeta]$. We know that the discriminant of S lies in the ring generated by its coefficients; thus it is an integer.

3) a) Every root x of S is a root of P different from 1. We have $P'(X) = pX^{p-1}$ and $P'(X) = S'(X)(X-1) + S(X)$, so $S'(x) = P'(x)/(x-1) = px^{p-1}/(x-1)$.

b) $D(S) = (-1)^{(p-1)(p-2)/2} \prod_{1\le i\le p-1} S'(\zeta^i)$, by §3.6. On the one hand,

$$(-1)^{(p-1)(p-2)/2} = ((-1)^{p-2})^{(p-1)/2} = (-1)^{(p-1)/2}$$

since $p-2$ is odd and $(p-1)/2$ is an integer.

On the other hand, $\prod_{1\le i\le p-1} S'(\zeta^i) = \prod_{1\le i\le p-1} p\zeta^{i(p-1)}/(\zeta^{i-1})$. In the numerator of this expression, we have $(\prod_{1\le i\le p-1} \zeta^i)^{p-1}$; the exponent of ζ in the part between parentheses is $\sum_{1\le i\le p-1} i = (p(p-1))/2$. As $\zeta^p = 1$, the numerator is thus p^{p-1}.

The denominator is given by

$$\prod_{1\le i\le p-1} (\zeta^i - 1) = (-1)^{p-1} \prod_{1\le i\le p-1} (1-\zeta^i) = S(1) = p.$$

Thus $d^2 = D(S) = (-1)^{(p-1)/2} p^{p-2}$.

4) a) If $p = 4k+1$, then $d^2 = p^{p-2}$, so $p/d^2 = 1/p^{p-1} = (1/p^{2k})^2$ and $\sqrt{p}/d = \pm(1/p^{2k})$ is rational.

If $p = 4k+3$, then $d^2 = -p^{p-2}$, so $p/d^2 = -(1/p^{p-1}) = -(1/p^{2k+1})^2$ and $\sqrt{p}/id = \pm(1/p^{2k+1})$ is rational.

b) First, $i = (\zeta_{4n})^n$ and $\zeta_n = (\zeta_{4n})^4$ show that $\mathbb{Q}[i, \zeta_n] \subset \mathbb{Q}[\zeta_{4n}]$. Then, as 4 and n are relatively prime, we see that i is of order 4 and ζ_n is of order n in $\mathbb{C}^*$, and $i\zeta_n$ is of order $\operatorname{lcm}(4, n) = 4n$ in $\mathbb{C}^*$, which proves that $i\zeta_n$ is a primitive $4n$-th root of unity, so we have shown the converse inclusion. Finally, $\mathbb{Q}[i, \zeta_n] = \mathbb{Q}[\zeta_{4n}]$.

c) If $p = 1 \bmod 4$, then part **a)** shows that $\sqrt{p}/d \in \mathbb{Q}$. As $d \in \mathbb{Q}[\zeta]$, we have $\sqrt{p} \in \mathbb{Q}[\zeta] = \mathbb{Q}[\zeta_p]$.

If $p = 3 \bmod 4$, then part **a)** shows that $\sqrt{p}/id \in \mathbb{Q}$. As $d \in \mathbb{Q}[\zeta_p]$, we have $\sqrt{p} \in \mathbb{Q}[i, \zeta_p[= \mathbb{Q}[\zeta_{4p}]$.

5) If $N > 0$, the decomposition of N as a product of primes shows that $\sqrt{N}$ is a product of roots of primes. Because each of these roots lies in a cyclotomic field, their product also lies in a cyclotomic field (indeed, given cyclotomic fields generated by m-th roots of unity m_i with $1 \leq i \leq r$, the cyclotomic field generated by the m-th root of unity $m = \operatorname{lcm}\{m_i; 1 \leq i \leq r\}$ will contain them all. This extends easily to negative integers N.

Solution to Exercise 9.10.

1) The inclusion is a consequence of Exercice 9.9.

2) L is a quadratic extension of $\mathbb{Q}$ contained in N; it is the only one since there is only one subgroup of index 2 in the cyclic group G.

3) G' is the subgroup of index 2 of G. It has $(p-1)/2$ elements, namely the σ_k for $k = a^{2r}$, $1 \leq r \leq (p-1)/2$.

4) The roots of S are the $\sigma_k(\zeta)$ for $\sigma_k \notin G'$; those of T are the $\sigma_k(\zeta)$ for $\sigma_k \notin G'$. We note that $T = \sigma_a(S)$. The irreducibility of S and T over L is a consequence of the fact that ζ is of degree $(p-1)/2$ over L. The constant term of S is $(-1)^{(p-1)/2}\zeta^N$ with $N = \sum_{1 \leq r \leq (p-1)/2} a^{2r} = 0 \bmod p$; thus it is 1 if $p = 1 \bmod 4$ and -1 if $p = 3 \bmod 4$.

5) a) If $p = 7$, then 3 is a generator of $(\mathbb{Z}/7\mathbb{Z})^*$ and its successive powers are 3, 2, 6, 4, 5, 1. We have $S(X) = (X-\zeta^2)(X-\zeta^4)(X-\zeta) = X^3 - \beta X^2 - (\beta+1)X - 1$. We compute $\beta = \zeta + \zeta^2 + \zeta^4$ by noting that the conjugate of β over $\mathbb{Q}[\sqrt{7}]$ is $\sigma_a(\beta) = \zeta^3 + \zeta^5 + \zeta^6$. As $\beta + \sigma_a(\beta) = -1$ and $\beta\sigma_a(\beta) = 2$, we see that $\beta^2 + \beta + 2 = 0$, which gives $\beta = (-1 + i\sqrt{7})/2$, taking into account that $\operatorname{Im}\beta > 0$.

We can determine T in the same way, and with $\beta' = (-1 - i\sqrt{7})/2$, we find

$$\Phi_7(X) = (X^3 - \beta X^2 - (\beta + 1)X - 1)(X^3 - \beta' X^2 - (\beta' + 1)X - 1).$$

b) If $p = 13$, then 2 is a generator of $(\mathbb{Z}/13\mathbb{Z})^*$, and we have

$$\begin{aligned} S(X) &= (X - \zeta^4)(X - \zeta^3)(X - \zeta^{12})(X - \zeta^9)(X - \zeta^{10})(X - \zeta) \\ &= X^6 - \gamma X^5 + 2X^4 - (1 + \gamma)X^3 + 2X^2 - \gamma X + 1. \end{aligned}$$

The computation of $\gamma = \zeta^2 + \zeta^5 + \zeta^6 + \zeta^7 + \zeta^8 + \zeta^{11}$ is done as above: we see that $\gamma^2 + \gamma - 3 = 0$, which gives $\gamma = (-1 + \sqrt{13})/2$, taking into account that $\gamma > 0$.

We can determine T similarly, and now, with $\gamma' = (-1 - \sqrt{13})/2$, we find

$$\begin{aligned} S(X) &= X^6 - \gamma X^5 + 2X^4 - (1 + \gamma)X^3 + 2X^2 - \gamma X + 1, \\ T(X) &= X^6 - \gamma' X^5 + 2X^4 - (1 + \gamma')X^3 + 2X^2 - \gamma' X + 1. \end{aligned}$$

10
Cyclic Extensions

After having studied extensions by roots of unity in Chapter 9, we now proceed to study extensions by roots of arbitrary elements of the base field, and consider in particular when such extensions have cyclic Galois group.

10.1 Cyclic and Abelian Extensions

DEFINITION. – A normal extension N of a field K contained in $\mathbb{C}$ is said to be *cyclic* if the Galois group $\mathrm{Gal}(N|K)$ is cyclic, and *abelian* if $\mathrm{Gal}(N|K)$ is abelian.

EXAMPLE. – The extension of a subfield K of $\mathbb{C}$ by a root of unity is abelian (see §9.5).

COMMENTARY. – Generally, we will use the term *cyclic* (resp. *abelian*) extension of a field K for a *Galois* extension N of K whose Galois group $\mathrm{Gal}(N|K)$ is cyclic (resp. abelian); for more details, see §15.6.

10.2 Extensions by a Root and Cyclic Extensions

PROPOSITION. – *Let $n \geq 1$ be an integer, ζ a primitive n-th root of unity in $\mathbb{C}$, K a subfield of $\mathbb{C}$ containing ζ, and a an element of K. Let b be a root of $X^n - a$ in $\mathbb{C}$.*

1) $K[b]$ is a cyclic extension of K of degree a divisor d of n, and $b^d \in K$.

2) In particular, if $X^n - a$ is irreducible over K, then $\mathrm{Gal}(K[b]|K)$ *is cyclic of order n.*

PROOF. –

1) The roots of $X^n - a$ in $\mathbb{C}$ are the n numbers $b\zeta^k, 0 \le k \le n-1$. As they are all elements of $K[b]$, $K[b]$ is a normal extension of K. Set $G = \mathrm{Gal}(K[b]|K)$. For every σ of G, $\sigma(b)$ is a conjugate of b over K, which can be written uniquely as $b\zeta^k$ avec $0 \le k \le n-1$. The map $\psi: G \to \mathbb{Z}/n\mathbb{Z}$ defined by $\psi(\sigma) = k$ is a group homomorphism, since if $\sigma(b) = b\zeta^k$ and $\sigma'(b) = b\zeta^{k'}$, then $(\sigma \circ \sigma')(b) = \sigma(b\zeta^{k'}) = b\zeta^{k+k'}$. It is injective, since if $\psi(\sigma) = 0$, then $\sigma(b) = b$, so $\sigma = \mathrm{id}$. It follows that because G is isomorphic to a subgroup of the cyclic group $\mathbb{Z}/n\mathbb{Z}$, it is itself cyclic of order a divisor d of n.

   Let σ be a generator of G and set $\sigma(b) = b\zeta^k$. As σ is of order d, k is of order d in $\mathbb{Z}/n\mathbb{Z}$, so $\sigma(b^d) = (b\zeta^k)^d = b^d\zeta^{kd} = b^d$. Because the element b^d is invariant under σ, it is invariant under every element G; thus it lies in K.

2) If $X^n - a$ is irreducible over K, $[K[b] : K] = n$ so $|G| = n$. ◊

EXAMPLE. – Consider the example of the field $K = \mathbb{Q}[j, \sqrt{2}]$, which contains the sixth roots of unity. The polynomial $X^3 - \sqrt{2}$ is the minimal polynomial of $b = \sqrt[6]{2}$ over K since $[K[b] : K] \cdot [K : \mathbb{Q}[\sqrt{2}] = [K[b] : \mathbb{Q}[b]].[\mathbb{Q}[b] : \mathbb{Q}[\sqrt{2}] = 6$ shows that b is of degree 3 over K. The group $\mathrm{Gal}(K[b]|K)$ is thus isomorphic to $\mathbb{Z}/3\mathbb{Z}$; its elements send b to b, jb, j^2b.

10.3 Irreducibility of $X^p - a$

PROPOSITION. – *Let p be a prime such that $p \ge 2$, K a subfield of $\mathbb{C}$, ζ a primitive p-th root of unity, and a an element of K.*

1) If K contains ζ, the polynomial $X^p - a$

- *either is irreducible in $K[X]$*
- *or factors as a product of linear factors in $K[X]$.*

2) If K does not contain ζ, the polynomial $X^p - a$

- *is either irreducible in $K[X]$*
- *or admits at least one root in K.*

PROOF. –

1) Proposition 2 shows that if b is a root of $X^p - a$ in $\mathbb{C}$, then $K[b]$ is a cyclic extension of K of degree a divisor d of p. If $d = p$, then $X^p - a$ is irreducible in $K[X]$; if $d = 1$, then $X^p - a$ factors as a product of linear factors in $K[X]$ (which are pairwise distinct since $X^p - a$ is prime to its derivative in $K[X]$, given that K has characteristic zero).

2) If $X^p - a$ is not irreducible in $K[X]$, then $X^p - a = P(X)S(X)$, where P and S are non-constant polynomials of $K[X]$.

   If b is a root of $X^p - a$ in $\mathbb{C}$, we have $X^p - a = \prod_{0 \leq k \leq p-1} (X - b\zeta^k)$ in $\mathbb{C}[X]$. The constant term of $P(X)$ is equal (up to sign) to a product c of terms of the form $b\zeta^k$; thus $c \in K$ and $c = b^r\zeta^s$, with $1 \leq r < p$. We have $c^p = b^{rp}\zeta^{sp} = a^r$. By Bézout's identity, there exist integers u and v such that $ur + vp = 1$; hence $a = a^{ur+vp} = c^{up}a^{vp} = (c^u a^v)^p$. As $c^u a^v \in K$, we see that $X^p - a$ has a root in K. ◊

10.4 Hilbert's Theorem 90

10.4.1 The Norm

DEFINITION. – Let K be a field, and let L be a normal extension contained in $\mathbb{C}$, of finite degree over K. Let $G = \mathrm{Gal}(L|K)$. For every $a \in L$, we define the norm of a over K to be the product $N_{L/K}(a) = \prod_{\sigma \in G} \sigma(a)$. When there is no risk of confusion, we simply write N for the norm. As $N(a)$ is invariant under every K-automorphism of L, we have $N(a) \in K$. If L is the normal closure of $K[a]$, $N(a)$ is the product of the conjugates of a over K. Finally, it is clear that $N(ab) = N(a)N(b)$.

The norm depends on the extension L: if L' is a normal extension of finite degree of K containing L, then $N_{L'/K}(a) = (N_{L/K}(a))^{[L':L]}$ for every $a \in L$.

The norm can be considered as a determinant (see Exercise 10.4).

EXAMPLES. – If $K = \mathbb{Q}$, then $a, b \in \mathbb{Q}$, and we have:

1) if $L = \mathbb{Q}[i]$, $N(a + ib) = (a + ib)(a - ib) = a^2 + b^2$;

2) if $L = \mathbb{Q}[j]$, $N(a + jb) = (a + jb)(a + j^2b) = a^2 - ab + b^2$.

3) if $L = \mathbb{Q}\left[\sqrt{2}\right]$, $N\left(a + b\sqrt{2}\right) = \left(a + b\sqrt{2}\right)\left(a - b\sqrt{2}\right) = a^2 - 2b^2$.

10.4.2 Hilbert's Theorem 90

THEOREM. – *Let K be a field, and let $L \subset \mathbb{C}$ be a cyclic extension of degree n of K. Let $G = \mathrm{Gal}(L|K)$, and let σ be a K-automorphism of L that generates G. For every x of L, we have the equivalence*

$$N(x) = 1 \iff \exists y \neq 0 \quad \text{such that} \quad x = \frac{y}{\sigma(y)}.$$

PROOF. – We have $G = \{\sigma^k; 0 \le k \le n-1\}$, so if $x = \dfrac{y}{\sigma(y)}$, then

$$N(x) = \prod_{0 \le k \le n-1} \sigma^k(x) = \frac{y}{\sigma(y)} \cdots \frac{\sigma^{n-1}(y)}{\sigma^n(y)} = 1$$

because $\sigma^n(y) = y$.

Conversely, suppose that $N(x) = 1$. The linear combination

$$\mathrm{id} + x\sigma + \ldots + \left[x\sigma(x) \ldots \sigma^{n-2}(x)\right] \sigma^{n-1}$$

of K-automorphisms is not identically zero (Dedekind's theorem; see §6.6.3). Let z be an element of L where it does not vanish; let y be its value at z. As $y = z + x\sigma(z) + \ldots + x\sigma(x) \ldots \sigma^{n-2}(x)\sigma^{n-1}(z) \neq 0$, we have

$$x\sigma(y) = x\sigma(z) + \cdots + x\sigma(x) \ldots \sigma^{n-1}(x)\sigma^n(z) = y - z + N(x)z = y,$$

which gives the result. ◇

COMMENTARY. – This theorem appears in a text by Hilbert entitled *Die Theorie der algebraischen Zahlkörper*, which first appeared in 1897, and whose French translation appeared in 1909 under the title *Théorie des corps de nombres algébriques.* The whole of the theory is remodeled and restructured there, in 200 pages and 169 numbered theorems.

10.5 Extensions by a Root and Cyclic Extensions: Converse

Let us now prove a converse of Proposition 10.2.

PROPOSITION. – *Let $n \ge 1$ be an integer, ζ a primitive n-th root of unity, K a field containing ζ, and $L \subset \mathbb{C}$ a cyclic extension of K of degree n and Galois group G with generator σ. Under these conditions, there exist $a \in K$ and $b \in L$ such that $b^n = a$ and $L = K[b]$. In particular, G is the Galois group of $X^n - a$ over K.*

PROOF. – Let us consider the norm map $N : L \to K$. We have

$$N(\zeta^{-1}) = (\zeta^{-1})^n = 1;$$

Hilbert's Theorem 90 implies that there exists $b \in L$ such that $\zeta^{-1} = b/\sigma(b)$, so that $\sigma(b) = b\zeta$. We have $\sigma^k(b) = b\zeta^k$ for $0 \leq k \leq n-1$, and the elements $b\zeta^k$ are pairwise distinct conjugates of b. Consequently, $[K[b] : K] = n$, hence $L = K[b]$. Moreover, $\sigma(b^n) = (b\zeta)^n = b^n$ shows that b^n is invariant under σ, so it is invariant under every element of G, which proves that $b^n \in K$, by §8.5. ◇

REMARK. – We can give a proof of this result that does not use Hilbert 90, but the eigenvalues of σ as a K-linear map from L to L (see Exercise 10.3). Here, also, the result remains true for an arbitrary field of arbitrary characteristic.

10.6 Lagrange Resolvents

10.6.1 Definition

Let n be an integer, $n \geq 1$, K a field containing the n-th roots of unity, and $L \subset \mathbb{C}$ a cyclic extension of K of Galois group G with generator σ. For every root of unity ε and every element x of L, the sum

$$(\varepsilon, x) = x + \varepsilon\sigma(x) + \cdots + \varepsilon^{n-1}\sigma^{n-1}(x)$$

is called a *Lagrange resolvent.*

COMMENTARY. – The history of the resolvents used by Lagrange in 1770, in particular in the study of third-degree equations, lies at the heart of the algebraic resolution of equations. Resolvents can be found, in varying forms, in the work of Euler (1750), Bézout (1765), Vandermonde (1770), and Gauss (around 1800). In the proof above, the application of Hilbert's Theorem 90 to ζ^{-1} leads to the linear combination $\mathrm{id} + \zeta^{-1}\sigma + \cdots + [\zeta^{-1}]^{n-1}\sigma^{n-1}$ and thus to a Lagrange resolvent.

10.6.2 Properties

With the notation of §6.1, we have:

1) $\sigma((\varepsilon, x)) = \varepsilon^{-1}(\varepsilon, x)$;

2) $(1, x) \in K$;

3) $(\varepsilon, x)^n \in K$;

4) $(\varepsilon, x)(\varepsilon^{-1}, x) \in K$;

5) $\sum_{\varepsilon \in \mu_n} \varepsilon^{-r}(\varepsilon, x) = n\sigma^r(x)$ for $0 \leq r \leq n-1$.

PROOF. –

1) We have

$$\begin{aligned}\sigma((\varepsilon,x)) &= \sigma(x)+\cdots+\varepsilon^{n-1}\sigma^n(x)\\ &= \varepsilon^{-1}[\varepsilon\sigma(x)+\cdots+\varepsilon^{n-1}\sigma^{n-1}(x)+x]\\ &= \varepsilon^{-1}(\varepsilon,x).\end{aligned}$$

2) As $\sigma(1,x)=(1,x)$, by 1), $(1,x)$ is invariant under σ, and so under every element of G. Thus, §8.5 gives the result.

3) $\sigma((\varepsilon,x)^n)=[\sigma((\varepsilon,x))]^n=[\varepsilon^{-1}(\varepsilon,x)]^n=(\varepsilon,x)^n$, by 1), which gives the result exactly as in 2).

4) We have

$$\begin{aligned}\sigma((\varepsilon,x)(\varepsilon^{-1},x)) &= \sigma((\varepsilon,x))\sigma((\varepsilon^{-1},x))=\varepsilon^{-1}(\varepsilon,x)\varepsilon(\varepsilon^{-1},x)\\ &= (\varepsilon,x)(\varepsilon^{-1},x)\end{aligned}$$

by 1), which again gives the result just as in 2).

5) Set $s_r=\sum_{\varepsilon\in\mu_n}\varepsilon^{-r}(\varepsilon,x)$.

We have $s_r=\sum_{\varepsilon\in\mu_n}\varepsilon^{-r}\sum_{0\le k\le n-1}\varepsilon^k\sigma^k(x)=\sum_{0\le k\le n-1}\sigma^k(x)\sum_{\varepsilon\in\mu_n}\varepsilon^{k-r}$.

Now, $\sum_{\varepsilon\in\mu_n}\varepsilon^{k-r}=n$ if $k=r$ and $\sum_{\varepsilon\in\mu_n}\varepsilon^{k-r}=0$ if $k\neq r$, since if ω is a primitive n-th root of unity, then

$$\sum_{\varepsilon\in\mu_n}\varepsilon^{k-r}=\sum_{0\le l\le n-1}(\omega^l)^{k-r}=\sum_{0\le l\le n-1}(\omega^{k-r})^l=\frac{1-(\omega^{k-r})^n}{1-\omega^{k-r}}=0.$$

This gives the result. ◊

10.7 Resolution of the Cubic Equation

In this section, we will show how the results of the preceding sections and of Chapter 8 guide the resolution of cubic equations.

A cubic equation can always be brought (by translation) to the form $x^3+px+q=0$, with $p,q\in\mathbb{C}$. Set $K=\mathbb{Q}(p,q,j)$; we need to adjoin the cube roots of unity because we will encounter a cyclic cubic extension.

Let a, b, c be the roots of the equation in $\mathbb{C}$. Recall (see VII.1 and III.6) that $K[a,b,c]=K[a,d]$ with $d=(a-b)(b-c)(c-a)$ and $d^2=-4p^3-27q^2$.

We know that the Galois group of $X^3 + pX + q$ is, in general, S_3, identified with the group of permutations of $\{a, b, c\}$; in what follows, we fix this identification once and for all. Let $L = I(A_3)$ be the field of invariants of the alternating group A_3, i.e. the group of even permutations of $\{a, b, c\}$. This group contains three elements: the identity, the 3-cycle $\sigma = (a \;\; b \;\; c)$ and its square $\sigma^2 = (a \;\; c \;\; b)$. As A_3 is a subgroup of index 2 of S_3, L is a quadratic extension of K and there exists an element $z \in L$ such that $z^2 \in K$ and $L = K[z]$.

Furthermore, $K[a, b, c]$ is a cyclic extension of L, since $K[a, b, c]$ is a normal extension of K, so it is a normal extension of L, and the alternating group $A_3 = \text{Gal}(K[a, b, c]|L)$ is a cyclic group of order three. By Proposition 10.5, there exists an element $z' \in K[a, b, c]$ such that $z'^3 \in L$ and $K[a, b, c] = L[z']$. The trellis of subgroups of the equation thus shows the existence of an intermediate extension which we will use to compute a, b, c in steps (Figure 10.1). To determine elements like z and z', we will use Lagrange resolvents and results from §10.6.

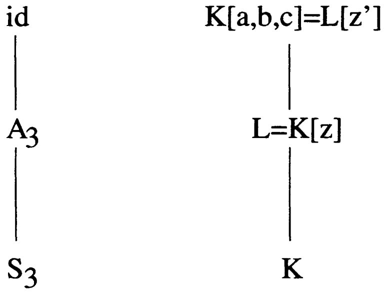


FIGURE 10.1.

To determine z, we use the discriminant d; the even permutations of $\{a, b, c\}$, namely id, σ, σ^2, leave d invariant, and an odd permutation like $(a \;\; b)$ transforms d into its conjugate $-d \neq d$. This shows that $d \in L$ and $d \notin K$, so $L = K[d]$.

To determine z', we follow the ideas of §10.4 and §10.5. We choose a cube root of unity, for example j. The linear combination of K-automorphisms $f = \text{id} + j\sigma + j^2\sigma^2$ is non-zero by Dedekind's theorem. It does not vanish at a, otherwise we would have $f(b) = j^2 f(a) = 0$, $f(c) = jf(a) = 0$, but as $f(1) = 0$, f would be zero. Consider $(j, a) = a + jb + j^2 c = f(a)$. We have $(j, a) \notin L$, since $\sigma(j, a) = j^2(j, a) \neq (j, a)$ and $(j, a)^3 \in L$, by Property 10.6.2 c); thus, (j, a) is a primitive element of the extension $K[a, b, c]$ of $K[d]$.

It remains to apply the techniques of Chapter 3 to compute the equation satisfied by $(j, a)^3 = (a + jb + j^2c)^3$. As

$$d = (a - b)(b - c)(c - a) = ab^2 + bc^2 + ca^2 - a^2b - b^2c - c^2a,$$

we find

$$\begin{aligned}(j,a)^3 &= a^3+b^3+c^3+3j(a^2b+b^2c+c^2a)+3j^2(ab^2+bc^2+ca^2)+6abc\\ &= a^3+b^3+c^3-\frac{3}{2}[a^2b+b^2c+c^2a+ab^2+bc^2+ca^2]-3\frac{i\sqrt{3}}{2}d+6abc\\ &= -\frac{27q}{2}-\frac{3i\sqrt{3}}{2}d.\end{aligned}$$

We obtain three values of (j,a), corresponding to the three possible values of a. Similarly, we find $(j^2,a)^3 = -(27q/2)+(3i\sqrt{3}/2)d$.

We need to determine the roots of the equation. By Property 10.6.2. 4), $(j,a)(j^2,a) \in L$:

$$\begin{aligned}(j,a)(j^2,a) &= (a+jb+j^2c)(a+j^2b+jc) = a^2+b^2+c^2-ab-bc-ca\\ &= -3p.\end{aligned}$$

Thus, we obtain three values of (j^2,a) corresponding to the three values of (j,a). Now, because $(1,a) = a+b+c = 0$, the formulas of 10.6.2 5) yield

$$\begin{aligned}3a &= (j,a)+(j^2,a),\\ 3b &= j^2(j,a)+j(j^2,a),\\ 3c &= j(j,a)+j^2(j^2,a).\end{aligned}$$

We recover Cardan's formulas this way, since

$$\left(\frac{(j,a)}{3}\right)^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4}+\frac{p^3}{27}},$$

etc.

10.8 Solution of the Quartic Equation

A quartic equation with complex coefficients can always be brought (by translation) to an equation of the form $x^4+px^2+qx+r=0$ with $p,q,r \in \mathbb{C}$. Set $K = \mathbb{Q}(p,q,r,j)$; again, we need to adjoin the cube roots of unity because we will encounter a cyclic extension of degree 3. Let a,b,c,d denote the roots of the equation in $\mathbb{C}$. We know that the Galois group of the equation is, in general, the group S_4 identified with the permutations of $\{a,b,c,d\}$; again, we fix such an identification once and for all. Let us show how knowing the Galois group guides the resolution of the fourth-degree equation.

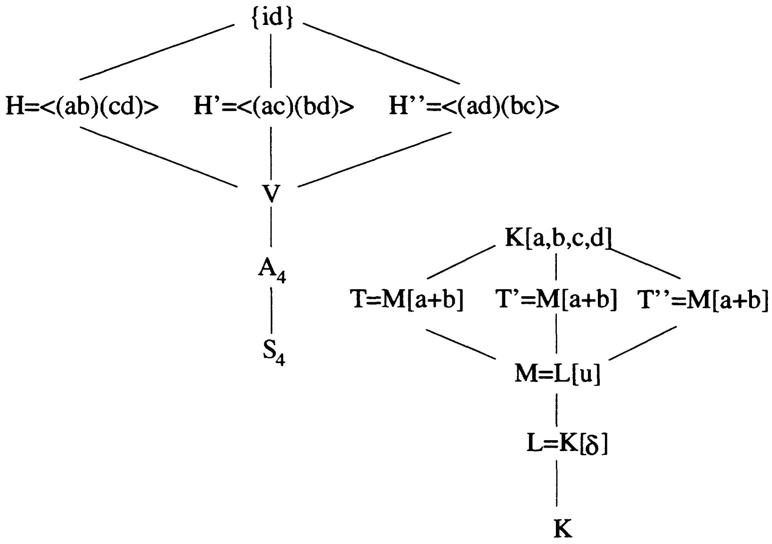


FIGURE 10.2.

Let A_4 be the alternating subgroup, and V the normal subgroup of order 4 generated by products of two disjoint transpositions (these are called *double transpositions*). Let H, H', H'' denote the three subgroups of V having two elements, and let L, M, T, T', T'' be the corresponding subfields of invariants. Figure 10.2 gives the Galois correspondence for the subgroups of S_4 just described, and their corresponding subfields.

As in §10.7, L is a quadratic extension of K and $L = K[\delta]$, where δ is a square root of the discriminant of the equation

$$\delta = (a-b)(a-c)(a-d)(b-c)(b-d)(c-d).$$

M is a cyclic extension of degree 3 of L, since V is a normal subgroup of index 3 of A_4. Lagrange's method for finding an element generating M over L is to consider

$$u = (a+b)(c+d), \qquad v = (a+c)(b+d), \qquad w = (a+d)(b+c)$$

(we can also work with the resolvents (i, a), $(-1, a)$, $(-i, a)$ or with $ab + cd, ac + bd$, $ad + bc$). The actions of V and A_4 over u, v, w are the desired ones: they are invariant under V but not under A_4 (recall that the elements of A_4 are 3-cycles or double transpositions), so they generate M. Moreover, considering the action of the 3-cycle $(a\ b\ c)$, we see that they are conjugates over L, so they are the roots of a cubic equation over L, which we can determine by computing $u + v + w = 2(ab + ac + ad + bc + bd + cd) = 2p$. Similarly,

$$\begin{aligned} uv + vw + wu &= p^2 - 4r, \\ uvw &= -q^2. \end{aligned}$$

The equation $y^3 - 2py^2 + (p^2 - 4r)y + q^2 = 0$ is called the resolvent equation of the original equation. As it is cubic, we know how to solve it (see §10.7).

Note that $[M : L] = 3$ and not 6; we can check by an easy computation that $(u-v)^2(v-w)^2(w-u)^2 = \delta^2$, so the discriminant of the resolvent lies in L.

Let us continue: $a + b \notin M$ since the element $(a \ \ c)(b \ \ d)$ of V modifies it; we do, of course, have $a + b \in I(H)$. Thus, $a + b$ is of degree 2 over M and $T = M[a + b]$; its conjugate is $c + d$, the image of $a + b$ under the permutation $(a \ \ c)(b \ \ d)$. As $a + b + c + d = 0$ and $(a + b)(c + d) = u$, we set $a + b = \sqrt{-u}$ and $c + d = -\sqrt{-u}$.

Similarly, $a + c = \sqrt{-v}$ and $b + d = -\sqrt{-v}, a + d = \sqrt{-w}$ and $b + c = -\sqrt{-w}$.

The numbers $\sqrt{-u}$, $\sqrt{-v}$, $\sqrt{-w}$ should not be selected independently. The (easily checked) equality $(a+b)(a+c)(a+d) = -q$ shows that we have the choice between two of the roots.

We finally obtain

$$\begin{aligned} 2a &= a+b+a+c+a+d = \sqrt{-u} + \sqrt{-v} + \sqrt{-w}, \\ 2b &= \sqrt{-u} - \sqrt{-v} - \sqrt{-w}, \\ 2c &= -\sqrt{-u} + \sqrt{-v} - \sqrt{-w}, \\ 2d &= -\sqrt{-u} - \sqrt{-v} + \sqrt{-w}. \end{aligned}$$

10.9 Historical Commentary

Lagrange was not the first to make the attempt to unify the methods for solving equations of degrees 2, 3, and 4. Tschirnhaus also tried; however, his ideas did not extend to equations of degree ≥ 5 (see Exercise 3.2).

Lagrange also wrote: "We can be assured that even if we succeeded in giving a general solution of the fifth degree equation and the following ones, we would have only algebraic formulas, precious in themselves, but not very useful for effective resolution...."

For further information on the methods of Lagrange, see for example the book by J.-P. Tignol (pp. 163–201) listed in the bibliography.

Exercises for Chapter 10

Exercise 10.1. Cyclic and abelian extensions

1) **a)** Show that a quadratic extension is cyclic.

b) Determine the set of elements x of $\mathbb{Q}[j]$ such that $\mathbb{Q}[x] = \mathbb{Q}[j]$ and $x^2 \in \mathbb{Q}$.

2) Let N be an abelian extension of a field K. Show that every intermediate extension L is an abelian extension of K.

3) Give an example of a non-cyclic abelian extension of $\mathbb{Q}$.

4) Let $a = \sqrt[4]{5}$, $b = a + ia$, and let N be the normal closure of $\mathbb{Q}[b]$ over $\mathbb{Q}$.

   a) Is N a cyclic extension of $\mathbb{Q}$?

   b) Give a strict subfield K of N such that $\mathrm{Gal}(N|K)$ is cyclic of order 4.

5) Determine the splitting field N of the polynomial $X^6 - 2$ over $\mathbb{Q}[j]$. Describe the elements of the Galois group $G = \mathrm{Gal}(N|\mathbb{Q}[j])$, and determine the structure of G.

Exercise 10.2. The splitting field of $(X^p - 2)(X^q - 2)$

1) Let $K = \mathbb{Q}[j]$, set $P(X) = (X^2 - 2)(X^3 - 2)$, and let N be the splitting field of P over K.

   a) Show that $N = K[a]$, where a is a suitable (non-integral) power of 2; determine $[N : K]$, and show that N is a cyclic extension of K.

   b) Give the trellis of intermediate extensions between K and N; are they all normal extensions of K?

2) Now let p and q be two distinct primes $n = pq$, ζ a primitive n-th root of unity, $K = \mathbb{Q}[\zeta]$, $P(X) = (X^p - 2)(X^q - 2)$, and N the splitting field of P over K. Show that N is a cyclic extension of K.

Exercise 10.3. Cyclic extensions without Hilbert's Theorem 90

Let K be a field contained in $\mathbb{C}$. A polynomial P of $K[X]$ is said to *split* if it is a product of linear factors in $K[X]$. Recall that if f is an endomorphism of a K-vector space such that there exists a split polynomial P in $K[X]$ with simple roots such that $P(f) = 0$, then f is diagonalisable.

1) Let $n \geq 1$ be an integer, ζ a primitive n-th root of unity, and K a field containing ζ. Let L be a cyclic extension of K of degree n, with Galois group G generated by σ. Consider σ as an endomorphism of the K-vector space L.

a) Show that the eignvalues of σ are n-th roots of unity, and that 1 is an eigenvalue of σ.

b) Show that σ is diagonalisable.

c) Deduce that 1 cannot be the only eigenvalue of σ.

d) Show that the eigenvalues of σ form a cyclic group isomorphic to the group μ_n of n-th roots of unity.

e) Show that there exists $a \in K$, $b \in L$ such that $b^n = a$ and $L = K[b]$.

2) Let $P(X) = X^3 + pX + q$ be a polynomial with coefficients in $\mathbb{C}$, irreducible over $K = \mathbb{Q}(p,q)$. Let a, b, c denote its roots in $\mathbb{C}$, and let d be a square root of its discriminant. Set $L = K[j,d]$, $N = L[a,b,c]$.

a) Show that $(1,a,b)$ is a basis of N over L.

b) Show that $G = \mathrm{Gal}(N|L)$ is cyclic.

c) Let σ be a generator of G. Determine the eigenvalues and eigenvectors of σ.

d) Check that we obtain Lagrange resolvents.

Exercise 10.4. The norm as determinant

Let $L \subset \mathbb{C}$ be a normal extension of a field K and a an element of L. Let $P(X) = \sum_{0 \leq k \leq n} a_k X^k$ be the minimal polynomial of a over K, and L' the normal closure of $K[a]$ in L. We write $m : L \to L$ for the map defined by $m(x) = ax$, and set $m' = m|L'$.

1) Check that m is K-linear.

2) **a)** Express $N_{L'/K}(a)$ in terms of the coefficients of P.

b) Show that $N_{L'/K}(a) = \det(m')$.

3) Deduce that $N_{L/K}(a) = \det(m)$.

Solutions to Some of the Exercises

Solution to Exercise 10.1.

1) a) We know that such an extension is normal and has Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

b) $\mathbb{Q}[j]$ is a cyclic extension of $\mathbb{Q}$, since it is a normal extension and its Galois group over $\mathbb{Q}$ is $\mathbb{Z}/2\mathbb{Z}$. Thus, there exists x such that $\mathbb{Q}[x] = \mathbb{Q}[j]$ and $x^2 \in \mathbb{Q}$. Writing $x = a + bj$, we see that $x^2 = a^2 + 2abj + b^2(-1 - j)$ is real if $2ab - b^2 = 0$. As b must be non-zero, it is necessary and sufficient that $b = 2a$. We find $x = a + 2aj = ai\sqrt{3}$ with $a \neq 0$. Thus, we have $x^2 = -3a^2 \in \mathbb{Q}$.

2) $\mathrm{Gal}(N|K)$ is an abelian group, and $\mathrm{Gal}(N|L)$ is a normal subgroup of it; thus L is a normal extension of K. Moreover, $\mathrm{Gal}(L|K)$ is a quotient of $\mathrm{Gal}(N|K)$, so it must be abelian, which gives the result.

3) Take the field $\mathbb{Q}\left[\sqrt{3}, \sqrt{2}\right]$; its Galois group over $\mathbb{Q}$ is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

4) a) The minimal polynomial of b over $\mathbb{Q}$ is $X^4 + 20$, whose roots are $\pm b$ and $\pm ib$. Thus we have $N = \mathbb{Q}\left[i, \sqrt[4]{5}\right]$. We see that $[N : \mathbb{Q}] = 8$ and $\mathrm{Gal}(N|\mathbb{Q})$ contains the elements σ and τ defined by $\sigma(i) = i$, $\sigma(a) = ia$, $\tau(i) = -i$, $\tau(a) = a$.

We note that $\sigma\tau \neq \tau\sigma$, since $\sigma\tau(a) = ia$ and $\tau\sigma(a) = -ia$. The group $\mathrm{Gal}(L|\mathbb{Q})$ is thus neither commutative nor cyclic.

b) Set $K = \mathbb{Q}[i]$; then K contains the fourth roots of unity. Thus, N is a cyclic extension of K, by §10.2, with Galois group isomorphic to $\mathbb{Z}/4\mathbb{Z}$ since $[N : \mathbb{Q}[i]] = 4$.

5) As $-j^2 = e^{\iota\pi/3}$ is a sixth root of unity, the splitting field is $N = \mathbb{Q}\left[\pm\sqrt[6]{2}, \pm j\sqrt[6]{2}, \pm j^2\sqrt[6]{2}\right] = \mathbb{Q}\left[\sqrt[6]{2}, j\right]$, so we have $[N : \mathbb{Q}] = 12, [N : \mathbb{Q}[j]] = 6$. A direct application of §10.2 shows that N is a cyclic extension $\mathbb{Q}[j]$, with Galois group isomorphic to $\mathbb{Z}/6\mathbb{Z}$. The elements of $\mathrm{Gal}(N|\mathbb{Q}[j])$ are defined by $\sigma(\sqrt[6]{2}) = (-j^2)^k\sqrt[6]{2}$, $0 \leq k \leq 5$.

Solution to Exercise 10.2.

1) a) We already saw, in part 2) of Exercise 4.5, that $a = 2^{1/6}$ is a primitive element of $\mathbb{Q}\left[\sqrt{2}, \sqrt[3]{2}\right]$. As $[N : \mathbb{Q}] = [\mathbb{Q}[a, j] : \mathbb{Q}[a]][\mathbb{Q}[a] : \mathbb{Q}] = 12$, it is clear that $[N : K] = 6$ and a is of degree 6 over K. As j is a sixth root of unity, Proposition 10.2 shows that N is a cyclic extension of K.

b) The only non-trivial subgroups of $\mathbb{Z}/6\mathbb{Z}$ are $\{0, 2, 4\}$ and $\{0, 3\}$; by the Galois correspondence, they correspond to extensions $K[\sqrt{2}]$ and $K[\sqrt[3]{2}]$, which are thus the only non-trivial intermediate extensions between K and N; note that they are all normal since $\mathbb{Z}/6\mathbb{Z}$ is abelian.

2) We have $N = K[2^{1/p}, 2^{1/q}]$. Set $a = 2^{1/n}$. As $a^q = 2^{1/p}$ and $a^p = 2^{1/q}$, we have $N \subset K[a]$. As there exist integers u and v such that $up + vq = 1$ by Bézout's identity, we have $2^{v/p}2^{u/q} = a$, which gives the converse inclusion and $N = K[a]$.

Solution to Exercise 10.3.

1) a) If λ is an eigenvalue of σ, there exists a non-zero $x \in L$ such that $\sigma(x) = \lambda x$. Thus $\sigma^k(x) = \lambda^k x$ for every integer $k \geq 0$; for $k = n$, we obtain $\lambda^n = 1$. Moreover, we have $\sigma(1) = 1$.

b) As $\sigma^n - I = 0$, we have $P(\sigma) = 0$ in $K[X]$, with $P(X) = X^n - 1$. As P is split over K because K contains the n-th roots of unity, the fact recalled above implies that σ is diagonalisable.

c) Because it is diagonalisable, σ cannot have 1 as its only eigenvalue, unless it is the identity, which is false.

d) If λ and μ are eigenvalues of σ and if x and y are the associated non-zero eigenvectors, we have $xy \neq 0$ and $\sigma(xy) = \lambda\mu xy$, $\sigma(x^{-1}) = \lambda^{-1}x^{-1}$. The eigenvalues of σ thus form a subgroup H of μ_n.

If H is strictly contained in μ_n, it is a cyclic group of order d dividing n, and thus contains only d-th roots of unity. As σ is diagonalisable, we have $\sigma^d =$id, which is false.

e) By **d)**, H contains ζ. Let b be a non-zero eigenvector of σ associated to ζ. We have $\sigma(b) = \zeta b$, so $\sigma(b^n) = \zeta^n b^n = b^n$; as $a = b^n$ is invariant under σ, it is invariant under all the elements of G, so it lies in K.

The conjugates of b are the $\sigma^k(b), 0 \leq k < n$, i.e. the $\zeta^k b$ for $0 \leq k < n$. They are all distinct, so b is of degree n over K and $L = K[b]$.

2) a) If b lies in the L-vector space generated by 1 and a, we see that $c \in L$ since $c = -a - b$. Thus $[N : L] \leq 2$, which is false.

b) By a), G is cyclic of order 3.

c) As σ induces a permutation of the roots of P, we have $\sigma(a) = b$ or c. Consider the first case. The matrix of σ in the preceding basis is given by

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix}.$$

The characteristic polynomial is $1 - X^3$, the eigenvalues are 1, j and j^2, and the corresponding eigenvectors are $(1, 0, 0)$, $(0, 1, -j)$ and $(0, 1, -j^2)$, i.e. $a - jb$ and $a - j^2b$.

d) As $(1 - j)(a - jb) = a + j^2b - ja - jb = a + j^2b + jc$ and similarly, $(1 - j^2)(a - j^2b) = a + jb + j^2c$, we find Lagrange resolvents up to the coefficients $1 - j$ and $1 - j^2$.

Solution to Exercise 10.4.

1) This is obvious.

2) a) $N_{L'/K}(a) = \displaystyle\prod_{\sigma \in \mathrm{Gal}(L'|K)} \sigma(a) = (-1)^n a_0.$

b) It is enough to compute the determinant of the matrix of m' in the basis $(a^k)_{0\le k\le n}$.

3) The determinant of m can be computed in a basis of the form

$$(a^k b_l)_{0\le k\le n, 0\le l\le r},$$

where $(b_l)_{0\le l\le r}$ is a basis of L over L'. We check that it is equal to $(\det(m'))^r$, which gives the result since $N_{L/K}(a) = (N_{L'/K}(a))^{[L:L']}$.

11
Solvable Groups

This chapter and the next one are devoted to the problem of resolving algebraic equations by radicals. Given a polynomial with coefficients in a field K, together with its splitting field N over K, the solvability of the equation $P(x) = 0$ by radicals can be expressed in terms of the existence of a particular sequence of intermediate extensions between K and N (see Chapter 12). By the Galois correspondence, this translates to a property of Galois group $\mathrm{Gal}(N|K)$. In this chapter, we introduce the groups having this special property, called *solvability.*

11.1 First Definition

A finite group G is *solvable* if it has a finite decreasing sequence $(G_i)_{0 \leq i \leq r}$ of subgroups such that

1) $G_0 = G \supset \cdots \supset G_r = \{e\}$;

2) G_{i+1} is a normal subgroup of G_i for $0 \leq i \leq r-1$;

3) G_i/G_{i+1} is commutative for $0 \leq i \leq r-1$.

EXAMPLES. –

1) An abelian group G is always solvable: it is enough to take $G_0 = G$ and $G_1 = \{e\}$.

2) S_3 is solvable: take $G_0 = S_3$, $G_1 = A_3$ and $G_2 = \{e\}$.

3) S_4 is solvable: take $G_0 = S_4$, $G_1 = A_4$, $G_2 = V$, and $G_3 = \{e\}$ where V is the subgroup consisting of the three *double transpositions* (products of two disjoint transpositions) and the identity.

4) A_n and S_n are not solvable for $n \geq 5$ (see §11.6).

5) Any p-group, and any group of order pq for distinct primes p and q, is solvable (see Exercise 11.3).

6) Any group whose order has only two prime divisors is solvable (Burnside's theorem, 1904).

11.2 Derived or Commutator Subgroup

Recall that a *commutator* in a group G is an element of the form $[a, b] = a^{-1}b^{-1}ab$, for any $a, b \in G$. The set of commutators of G generates a subgroup of G called the *commutator subgroup* of G, or the *derived subgroup* of G. We denote it by $D(G)$.

If $f : G \to G'$ is a group homomorphism, we have

$$f(D(G)) = D(f(G)) \subset D(G') \qquad \text{because} \qquad f[x, y] = [f(x), f(y)].$$

Recall that $D(G)$ is a normal subgroup of G, and even a characteristic subgroup of G, i.e. a subgroup stable under every automorphism of G (not only inner automorphisms).

Finally, let us recall a property that will be quite useful later on: for every normal subgroup H of G, $H \supset D(G)$ is abelian if and only if G/H is abelian.

11.3 Second Definition of Solvability

PROPOSITION. – *A finite group G is solvable if the sequence $D^i(G)$ defined inductively by $D^0(G) = G$ and for $i \geq 0$, $D^{i+1}(G) = D(D^i(G))$, eventually stabilizes at $\{e\}$, i.e. if there exists an integer s such that $D^s(G) = \{e\}$ (so that $D^i(G) = \{e\}$ for all $i \geq s$).*

PROOF. – Assume that G is solvable (as defined in §11.1). Then, by induction, we have $D^i(G) \subset G_i$. Indeed, this is clear for $i = 0$, and if we assume that for some integer i, G_i/G_{i+1} is abelian, then we obtain $G_{i+1} \supset D(G_i) \supset D(D^i(G)) = D^{i+1}(G)$. As $G_r = \{e\}$, we have $D^r(G) = \{e\}$.

Conversely, the sequence $D^i(G)$ is a sequence satisfying the conditions of the first definition, since conditions 1) and 2) are obvious, and also because

the fact that $D^{i+1}(G) = D(D^i(G))$ is normal in G_i shows that the quotient $D^i(G)/D^{i+1}(G)$ is commutative for every i. ◇

11.4 Examples of Solvable Groups

PROPOSITION. – *The following groups are solvable:*

1) a subgroup of a solvable group;

2) a quotient of a solvable group by a normal subgroup;

3) an extension of a solvable group by a solvable group;

4) a finite product of solvable groups.

PROOF. –

1) Let H be a subgroup of a solvable group G. We have $D^i(H) \subset D^i(G)$ for every $i \geq 0$. As G is solvable, there exists an integer r such that $D^r(G) = \{e\}$, so $D^r(H) = \{e\}$, which gives the result.

2) Let K be a normal subgroup of a solvable group G, and let $p : G \to G/K$ be the canonical homomorphism. We have $p(D(G)) = D(p(G)) = D\left(G/K\right)$, so by induction, we have $p(D^i(G)) = D^i\left(G/K\right)$ since $p(G) = G/K$. If $D^r(G) = \{e\}$, then $D^r\left(G/K\right) = \{e\}$, which gives the result.

3) Let $\{e\} \to K \xrightarrow{i} G \xrightarrow{p} H \to \{e\}$ be an exact sequence of groups, with K and H solvable (we say that G is an extension of K by H, or an extension of H by K; it depends on who is writing). There exists r such that $D^r(H) = \{e\}$, so $p(D^r(G)) = \{e\}$; hence $D^r(G) \subset i(K)$. There exists s such that $D^s(K) = \{e\}$ so $D^{r+s}(G) \subset i(D^s(K)) = \{e\}$, which gives the result.

4) It suffices to note that the product of two solvable groups H and K is solvable since $H \times K$ is an extension of H by K. Indeed, the sequence $\{e\} \to K \xrightarrow{i} H \times K \xrightarrow{p} H \to \{e\}$ is exact with $i(k) = (e, k)$ and $p(h, k) = h$. ◇

11.5 Third Definition

PROPOSITION. – *A finite group G is solvable if and only if there exists a finite decreasing sequence $(H_j)_{0 \leq j \leq r}$ of subgroups of G such that*

1) $H_0 = G \supset \cdots \supset H_r = \{e\}$;

2) H_{j+1} is a normal subgroup of H_j for $0 \leq j \leq r-1$;

3) H_j/H_{j+1} is cyclic of prime order for $0 \leq j \leq r-1$.

PROOF. – A group satisfying the above properties is solvable; this is clear using the first definition of solvability. Let us show the converse. Take a sequence $(G_i)_{0 \leq i \leq r}$ of subgroups of G satisfying the conditions of the first definition. For every i, $0 \leq i \leq r-1$, construct by induction a sequence (K_j) of intermediate groups between G_i and G_{i+1} : $K_0 = G_i$, and K_{j+1} is a maximal normal subgroup of K_j containing G_{i+1}. The sequence (K_j) is decreasing, and finite because G is finite. Because the normal subgroups of K_j/K_{j+1} are in bijection with the normal subgroups of K_j containing K_{j+1}, K_j/K_{j+1} is a group that has no proper normal subgroup, i.e. a simple group. Moreover, K_j/K_{j+1} is a subgroup of G_i/G_{i+1}. Thus, it is abelian, and consequently, it is cyclic of prime order. Putting together the sequences (K_j) obtained for each i, we obtain the result. ◇

11.6 The Group A_n Is Simple for $n \geq 5$

11.6.1 Theorem

For $n \geq 5$, the alternating group A_n is simple (i.e. it has no normal subgroups except for itself and the identity) and non-solvable; the group S_n is also non-solvable.

COMMENTARY. – This fundamental theorem is due to Galois. One can show directly that A_n is not a solvable group (see §11.6.2).

PROOF. – Let $n \geq 5$. Recall (see Exercise 11.1) that A_n is generated by the set of 3-cycles or by the set of double transpositions. Let us show that two 3-cycles $\sigma = (a \;\; b \;\; c)$ and $\sigma' = (a' \;\; b' \;\; c')$ are conjugate in A_n. There exists α in S_n such that $\alpha(a) = a'$, $\alpha(b) = b'$, $\alpha(c) = c'$. If α belongs to A_n, the equality $\alpha\sigma\alpha^{-1} = \sigma'$ shows that the two 3-cycles are conjugate in A_n; we obtain the same result if α does not belong to A_n, by changing α to $\beta = \alpha \circ (d \;\; e)$ where d and e lie in the complement of $\{a, b, c\}$. Similarly, we see that two double transpositions $(a \;\; b)(c \;\; d)$ and $(a' \;\; b')(c' \;\; d')$ are conjugate in A_n, by taking any permutation $\alpha \in S_n$ such that $\alpha(a) = a'$, $\alpha(b) = b'$, $\alpha(c) = c'$, $\alpha(d) = d'$. If α does not belong to A_n, set $\beta = \alpha \circ (a \;\; b)$.

Let H be a normal non-trivial subgroup of A_n. Let us show that H always contains a 3-cycle or a double transposition. By the above, it will contain all of them, and therefore be equal to A_n.

Let σ be an element of H different from the identity element e, and let $\sigma_1 \ldots \sigma_k$ be its decomposition into a product of disjoint cycles, indexed so that the sequence of lengths $l(\sigma_i)$ of these cycles is decreasing.

1) Assume that $l(\sigma_1) = r > 3$. Set

$$\sigma_1 = (a_1 \dots a_r) \text{ and } \sigma' = (a_1 \ a_2 \ a_3)\sigma(a_1 \ a_2 \ a_3)^{-1}.$$

We have

$$\begin{aligned} \sigma^{-1}\sigma &= (a_1 \dots a_r)^{-1}(a_1 \ a_2 \ a_3)(a_1 \dots a_r)(a_1 \ a_2 \ a_3)^{-1} \\ &= (a_r \ a_1 \ a_2)(a_1 \ a_3 \ a_2) \\ &= (a_1 \ a_3 \ a_r). \end{aligned}$$

Then σ' lies in H, because H is normal in A_n, so $\sigma^{-1}\sigma' = (a_1 \ a_3 \ a_r)$ lies in H; H contains a 3-cycle, so $H = A_n$.

2) Assume that $l(\sigma_1) = 3$ and $l(\sigma_i) = 2$ for $i > 1$. Then H contains the 3-cycle σ^2, so $H = A_n$.

3) Assume that $l(\sigma_1) = l(\sigma_2) = 3$. Set $\sigma_1 = (a \ b \ c)$, $\sigma_2 = (x \ y \ z)$, and $\sigma' = (b \ c \ x)\sigma(b \ c \ x)^{-1}$. Because $\sigma^{-1}\sigma'$ lies in H and $\sigma^{-1}\sigma' = (a \ b \ x \ c \ z)$, we can conclude using part a).

4) Assume that $l(\sigma_i) = 2$ for $i = 1, \dots, k$. Set $\sigma_1 = (a \ b)$, $\sigma_2 = (c \ d)$, and $\sigma' = (b \ c \ d)\sigma(b \ c \ d)^{-1}$. Because $\sigma^{-1}\sigma'$ lies in H and $\sigma^{-1}\sigma' = (a \ d)(b \ c)$, H contains a double transposition, so $H = A_n$.

   In every case, $H = A_n$; thus A_n is a simple group. As it is not commutative, it is not solvable, and by Proposition 11.4, S_n is also non-solvable. ♢

11.6.2 A_n Is Not Solvable for $n \geq 5$, Direct Proof

PROPOSITION. – *A_n is not solvable for $n \geq 5$.*

PROOF. – The proof consists in showing that the normal subgroup $D(A_n)$ is equal to A_n. Because A_n is generated by the 3-cycles (see Exercise 11.1), it suffices to show that every 3-cycle $(a \ b \ c)$ belongs to $D(A_n)$. Let d and e be two elements of $\{1, \dots, n\}$, different from a, b, c; then

$$[(a \ c \ d), (b \ c \ e)] = (a \ d \ c)(b \ e \ c)(a \ c \ d)(b \ c \ e) = (a \ b \ c). \quad ♢$$

11.7 Recent Results

The classification of all finite simple groups was completed in 1981. Galois discovered the first examples of these, namely, the alternating groups A_n for $n \geq 5$. Émile Mathieu discovered others in 1861. Beginning with a lecture by Richard Brauer at the International Congress of Mathematicians in 1954,

together with seminal work of Claude Chevalley from the same period, the proof that the list of known finite simple groups was actually a complete list represents an enormous effort on the part of the mathematical community. Counted all together, the different parts of the proof fill nearly 10,000 pages; it is the longest proof on record. Given that even the best mathematicians make errors every 50 pages or so.....

Certain simple groups fall naturally into some infinite series, whereas others, called sporadic, seem to be the only ones of their kind. Among the sporadic simple groups, the most famous and largest one is known as the monster (or sometimes, the friendly giant). It possesses spectacularly beautiful properties; its order is equal to $2^{46} \times 3^{20} \times 5^9 \times 7^6 \times 11^2 \times 13^3 \times 17 \times 19 \times 23 \times 29 \times 31 \times 41 \times 47 \times 59 \times 71$, which is roughly 10^{54}.

The proofs of theorems concerning solvable groups are also sometimes extremely long. In 1963, Walter Feit and John Thompson published a famous 255 page proof of the theorem "All finite groups of odd order are solvable."

Exercises for Chapter 11

The first exercises recall basic properties of permutation groups.

Exercise 11.1. The permutation groups S_n and A_n

1) The conjugate of a cycle.

Let n be an integer, σ a permutation of $\{1, \dots, n\}$, and $(x_1, \dots, x_k)$ a k-cycle of S_n, i.e. the permutation associating x_{i+1} to x_i for $i = 1, \dots, k-1$, x_1 to x_k and leaving the other elements of $\{1, \dots, n\}$ fixed. Show that $\sigma(x_1, \dots, x_k)\sigma^{-1} = (\sigma(x_1), \dots, \sigma(x_k))$.

2) Let $n \geq 3$ be an integer. Knowing that S_n is generated by the set of transpositions of $\{1, \dots, n\}$, show that S_n is generated by the following sets of permutations:

- **a)** the set of transpositions $(1\ \ 2), \dots, (1\ \ n)$;
- **b)** the set of transpositions $(1\ \ 2), (2\ \ 3), \dots, (n-1\ \ n)$;
- **c)** the set of two permutations $(1\ \ 2)$ and $(2\ \ 3 \dots n)$;
- **d)** the set of two permutations $(1\ \ 2)$ and $(1 \dots n)$;
- **e)** the set consisting of an arbitrary transposition and an arbitrary p-cycle σ.

3) Let $n \geq 3$ be an integer.

a) Show that the product of two distinct transpositions of S_n is either a 3-cycle or a product of two 2-cycles. Deduce that A_n is generated by the set of 3-cycles of S_n.

b) Show that for $n \geq 3$, A_n is generated by the set $\{(1\ \ 2\ \ 3), \ldots, (1\ \ 2\ \ n)\}$.

c) Show that for $n \geq 5$, A_n is generated by the set of permutations known as double transpositions, i.e. permutations of the form $(a\ \ b)(c\ \ d)$ with a, b, c, d pairwise distinct. Show that this result is false for $n = 3, 4$.

d) Show that, for every $n \geq 1$ and every odd integer k with $k \leq n$, A_n is generated by the k-cycles, by showing that every 3-cycle is a product of two k-cycles.

4) Take an action of S_n on a set E. Let p be the largest prime number less than or equal to n. Show that the orbits for this action have cardinal equal to 1, 2, or a number greater than or equal to p.

Exercise 11.2. The groups A_4 and S_4

1) Let G be a subgroup of A_4 containing two 3-cycles defined over distinct subsets of $E = \{1, 2, 3, 4\}$. Show that $G = A_4$.

2) a) Show that the elements of A_4 different from the identity element are eight 3-cycles and three double transpositions.

b) Show that A_4 has a unique normal subgroup, describe it, and show that it is normal in S_4.

3) Show that A_4 is the only subgroup of order 12 in S_4.

4) Find the transitive subgroups of A_4 and S_4.

Exercise 11.3. Examples of solvable groups

1) Show that a p-group is solvable.

2) Show that a group G of order pq for distinct primes p and q is solvable.

3) Show that a group G of order pqr for distinct primes p, q, and r is solvable.

4) Show that a group G of order p^2q for distinct primes p, q is solvable.

Exercise 11.4. Transitive and solvable subgroups of S_p

Let p be a prime. We know that $(\mathbb{Z}/p\mathbb{Z}, +, .)$ is a finite field with p elements. Let $E = \{0, \dots, p-1\}$ denote the set of its elements, and (for this exercise) consider S_p as the group of permutations of E.

Let $\mathrm{GA}(p)$ denote the group of bijective affine maps from $\mathbb{Z}/p\mathbb{Z}$ to itself, i.e. the maps $f_{a,b} : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ defined by $f_{a,b}(x) = ax + b$, with $a \neq 0$, $a, b \in \mathbb{Z}/p\mathbb{Z}$. Set $t = f_{1,1}$ and $m_a = f_{a,0}$. We will show that a subgroup G of S_p having the following properties:

1) the action of G on E is transitive,

2) G is solvable,

is conjugate to a subgroup H of $\mathrm{GA}(p)$, i.e. of the form $\sigma H \sigma^{-1}$ for a permutation σ of S_p; we will also prove the converse.

1) The group $\mathrm{GA}(p)$

a) Show that $m_a t = t^a m_a$.

b) Show that every element of $\mathrm{GA}(p)$ can be written uniquely in the form $t^b m_a$, with $1 \leq a \leq p-1$, $0 \leq b \leq p-1$.

Deduce that $|\mathrm{GA}(p)| = p(p-1)$.

c) Show that $\langle t \rangle$ is a normal subgroup of $\mathrm{GA}(p)$.

d) Show that $\mathrm{GA}(p)$ is transitive and solvable.

2) Let G be a transitive subgroup of S_p. Show that a normal subgroup $H \neq \{\mathrm{id}\}$ of G acts transitively on E.

3) **a)** Let G be a solvable subgroup of S_p acting transitively on E. Thus, we assume that there exists a finite decreasing sequence $(H_j)_{0 \leq j \leq r}$ of subgroups of G, satisfying the conditions of definition 11.5.

Show that H_{r-1} is conjugate to the group $\langle t \rangle$.

b) Deduce that G is conjugate to a subgroup of S_p containing t.

4) Let $\sigma \in S_p$ be such that $\sigma t \sigma^{-1} \in \mathrm{GA}(p)$. Show that $\sigma \in \mathrm{GA}(p)$.

5) Show that a group having properties **1)** and **2)** is of the stated form.

6) Let G be a transitive subgroup of S_p.

a) Show that if G is solvable, the only permutation of G having at least two fixed points is the identity.

b) Now let us prove the converse. By counting the elements of G that have a fixed point, show that there exists an element $\tau \in G$ that has no fixed point. Show that τ is a p-cycle. Conclude.

COMMENTARY. – These results are due to Galois. Later (see Exercise 12.3), we will prove the main result on equations that he deduced from them.

Solutions to Some of the Exercises

Partial solution to Exercise 11.1.

1) Set $\alpha = \sigma(x_1, \ldots, x_k)\sigma^{-1}$ and $\beta = (\sigma(x_1), \ldots, \sigma(x_k))$. We see that $\alpha(y) = \beta(y)$ in each of the two cases $y \notin \{\sigma(x_1), \ldots, \sigma(x_k)\}$ and $y \in \{\sigma(x_1), \ldots, \sigma(x_k)\}$.

2) d) Using the equalities

$$(1 \ldots n)^k (1\ \ 2)(1 \ldots n)^{-k} = (k+1\ \ k+2) \quad \text{for} \quad k = 1, \ldots, n-2,$$

we find ourselves in the situation of **b)**.

e) Let $(i\ \ j)$ denote the transposition; there exists an integer k such that $\sigma^k(i) = j$. If we set $\tau = \sigma^k$, then via the bijection φ defined by $\varphi(1) = i, \varphi(2) = j, \varphi(r+1) = \tau^r(i)$ for $2 \leq r \leq n-1$, we return to the previous situation.

3) d) The k-cycles are even permutations when k is odd, and they generate the set of 3-cycles, via the formula

$$(a_1\ \ a_2\ \ a_3) = (a_2\ \ a_1\ \ a_3\ \ a_4 \ldots a_k)(a_k \ldots a_4\ \ a_3\ \ a_2\ \ a_1).$$

4) The result is clear if $p = 2$, so let p be an odd prime, and take $x \in E$. For every p-cycle σ, the orbit of x under the action of $\langle\sigma\rangle$ has either one or p elements. If for every p-cycle σ, the orbit of x under the action of $\langle\sigma\rangle$ has only one element, then the orbit x under the action of A_n has only one element by **3) d)**, so the orbit of x under the action of S_n has at most two elements.

Partial solution to Exercise 11.2.

4) The order of a transitive subgroup G of A_4 is a multiple of 4, which is the order of the unique orbit, and it divides 12, so it is equal to 4 or 12. If it is 12, then $G = A_4$. If it is 4, then G is the subgroup generated by the double transpositions.

Similarly, a transitive subgroup G of S_4 has order a multiple of 4 and a divisor of 24, so it is equal to 4, 8, 12 or 24. If it is 24, then $G = S_4$, and if

it is 12, then $G = A_4$. If it is 4, then G can be the subgroup generated by the double transpositions, but also one of the three subgroups generated by a 4-cycle. If it is 8, then G is a Sylow 2-subgroup of S_4, i.e. one of the three subgroups isomorphic to the dihedral group described in §8.7.2.

Solution to Exercise 11.3.

1) If G is a p-group, we know that its order is of the form p^n. Let us use induction on n. If $n = 1$, then $G \simeq (\mathbb{Z}/p\mathbb{Z}, +)$, and the result is clear. Suppose the result holds for every p-group of order p^k with $k < n$, and let G be a p-group of order p^n. The center $Z(G)$ of G is a non-trivial abelian subgroup of G, so it is solvable. As $Z(G)$ is normal in G, the quotient $G/Z(G)$ is a p-group, solvable by the induction hypothesis. We conclude that G is solvable by Proposition 11.4 3).

2) Suppose that $p > q$. The number m_p of Sylow p-subgroups of G divides pq and is equal to 1 mod p. Thus, $m_p = 1$ and G has a unique Sylow p-subgroup H. We know that H is solvable and normal in G, and that the quotient G/H is solvable, so we conclude that G is solvable by Proposition 11.4 3).

3) Suppose that $p > q > r$ and G does not have any normal subgroups. Then by the Sylow theorems, we find:

a) $m_p = 1$ mod p, $m_p > 1$ and $m_p | pqr$, so $m_p = qr$;
b) $m_q = 1$ mod q, $m_q > 1$ and $m_q | pqr$, so $m_q \geq p$;
c) $m_r = 1$ mod r, $m_r > 1$ and $m_r | pqr$, so $m_r \geq q$.

Now, Sylow l-subgroups for distinct primes $l = p, q, r$ have trivial intersection, so we find that

$$|G| \geq qr(p-1) + p(q-1) + r(q-1) + 1 > pqr.$$

This contradiction shows that G must have a normal subgroup of prime order, so it must be solvable. Denote it by H. The group G/H is solvable by **2)**, and we can thus again use Proposition 11.4 3) to conclude.

4) If $p > q$, we see that $m_p = 1$, G has a normal subgroup H of order p^2, so solvable, by **1)**, and the quotient G/H is of order q and is also solvable. Again, we can conclude using §9.4 3).

Let $p < q$, and assume that G has no normal subgroups. The Sylow theorems give $m_p = 1$ mod p, $m_p > 1$, and $m_p | p^2 q$, so $m_p = q$. But they also give $m_q = 1$ mod q, $m_q > 1$, and $m_q | p^2 q$, so $m_q = p^2$. As two Sylow l-subgroups for distinct primes $l = p, q$ have trivial intersection, we find

$$|G| \geq q(p^2 - 1) + p^2(q-1) + 1 > p^2 q.$$

This contradiction shows that G must have a normal subgroup H of order p^2 or q. Because H is solvable, the group G/H is also solvable, and once again we conclude using §9.4 3).

Solution to Exercise 11.4.

1) a) This follows from the fact that $a(x+1) = ax + a$. Note that t is the p-cycle $(0\,1 \dots p-1)$.

b) As $f_{a,b} = t^b m_a$, it suffices to check that if $ax + b = a'x + b'$ for every $x \in \mathbb{F}_p$, then $a = a'$ and $b = b'$, which is easy.

c) Part **a)** shows that $m_a t m_a^{-1} = t^a$, which suffices since the m_a and t generate $\mathrm{GA}(p)$.

d) The quotient $\mathrm{GA}(p)/\langle t \rangle$ is commutative since the representatives of the classes are m_a's, which commute with each other. Thus, it is solvable. The same holds for $\mathrm{GA}(p)$ and its subgroups, by Proposition 11.4.

2) Let x and $y \in E$. As G is transitive, there exists $f \in G$ such that $f(x) = y$; for every $h \in H$, we have $f^{-1}hf \in H$, so $f^{-1}(O_H(y)) \subset O_H(x)$. Consequently, $|O_H(x)| = |O_H(y)|$. Under the action of H, E is thus the union of r disjoint orbits having the same number of elements s. As $s > 1$ (because $H \neq \{\mathrm{id}\}$), $p = rs$, so that we must have $s = p$ and $r = 1$. This proves the result.

3) a) By the preceding question, the groups H_i for $i = 0, \dots, r-1$ act transitively on E. The only possibility for H_{r-1} is a cyclic group generated by a p-cycle c. If $c = (x_0 \dots x_{p-1})$, and if we define $\varphi : E \to E$ by $\varphi(x_i) = i$, then $\varphi c \varphi^{-1} = t$.

b) $\varphi G \varphi^{-1}$ answers the question.

4) If $\sigma t \sigma^{-1} = t^b m_a$, we see, by an easy computation, that $\sigma t^k \sigma^{-1} = t^n m_{a^k}$ for $k \geq 1$, with $n = \sum_{0 \leq i \leq k-1} a^i b$. If $k = p-1$ and $a \neq 1$, we find that $n = 0 \bmod p$; hence, $\sigma t^{p-1} \sigma^{-1} = \mathrm{id}$. It follows that $t^{p-1} = \mathrm{id}$, which is absurd. Thus, we have $a = 1$ and $\sigma t \sigma^{-1} = t^b$, i.e. $\sigma t = t^b \sigma$. For every $i \in E$, we thus have $\sigma(i+1) = \sigma(i) + b$, hence $\sigma = t^{\sigma(0)} m_b$ which indeed lies in $\mathrm{GA}(p)$.

5) Let G have the two properties. By **3)**, there exists φ such that $\varphi G \varphi^{-1}$ contains t. As $\varphi H_{r-1} \varphi^{-1} = \langle t \rangle$ is a normal subgroup of $\varphi H_{r-2} \varphi^{-1}$, part **4)** shows that $\varphi H_{r-2} \varphi^{-1} \subset \mathrm{GA}(p)$. For the same reasons, $\varphi H_i \varphi^{-1} \subset \mathrm{GA}(p)$ for $0 \leq i \leq r-1$, which gives the result.

6) a) If G is solvable, it is conjugate to a subgroup Γ of $\mathrm{GA}(p)$. As the only element of $\mathrm{GA}(p)$ having at least two fixed points is the identity, the same holds for G.

b) For every $i \in \{0, \dots, p-1\}$, let $O(i)$ denote the orbit of i under G, and $S(i)$ the stabilizer of i; set $q = |S(0)|$. Because G is transitive, $O(i) = \{0, \dots, p-1\}$ and $|G| = |O(i)||S(i)|$ show that $|S(i)| = q$ for every i. By the hypotheses, G is the disjoint union of the $S(i) - \{\mathrm{id}\}$, together

with the set A of elements having no fixed points, and $\{\text{id}\}$. Thus $|A| = pq - p(q-1) - 1 = p - 1$, which proves the existence of τ.

Let n be the order of τ. For every $k < n$, $\tau^k \in A$ since if τ^k fixes i, it also fixes $\tau(i)$, which is impossible. Thus, the orbits under the action of $\langle\tau\rangle$ have the same cardinal n. As $\{0, \ldots, p-1\}$ is the disjoint union of these orbits, we see that n divides p. Consequently, $n = p$, τ is a p-cycle and $A \cup \{\text{id}\} = \langle\tau\rangle$.

Up to conjugation, we can assume that $\tau = t$. If $\sigma \in G$, $\sigma t \sigma^{-1}$ has no fixed points (otherwise t would), so $\sigma t \sigma^{-1} \in \langle t \rangle$ and by **4)**, we show that $G \subset \text{GA}(p)$. Thus, G is solvable.

12

Solvability of Equations by Radicals

Using the correspondence constructed in the preceding chapters, together with group-theoretic results, Galois obtained his famous criterion of *solvability by radicals.* "This material is so entirely new that new names and new characters are necessary to express it," he wrote, adding later that the true value of his criterion is essentially theoretical, as it is often impossible to compute the Galois group of a given polynomial: "In a word, the computations are not practicable." However, he adds, the applications generally lead to "equations all of whose properties are known beforehand," so that the computations are possible, as in Chapters 9 and 10.

12.1 Radical Extensions and Polynomials Solvable by Radicals

12.1.1 Radical Extensions

DEFINITION. – A field $L \subset \mathbb{C}$ is said to be a *radical extension* of a field K if there exists a tower $(K_i)_{0 \leq i \leq r}$, called a *radical tower*, of extensions of K such that for each $i = 0, \ldots, r-1$, K_{i+1} is an extension of K_i by a root of an element of K_i. In other words, we have

$$K_0 = K \subset \ldots \subset K_i = K[a_1, \ldots, a_i] \subset \ldots \subset L = K_r = K[a_1, \ldots, a_r];$$

hence, for each $i = 1, \ldots, r$, there exists an n_i such that $(a_i)^{n_i} \in K_{i-1}$.

EXAMPLE. – $\sqrt[12]{\sqrt[3]{1+\sqrt[5]{-7}+\sqrt{-5}}}$ belongs to a radical extension of $\mathbb{Q}$ (this formula actually defines 360 distinct complex numbers!)

12.1.2 Polynomials Solvable by Radicals

DEFINITION. – A polynomial $P(X) \in K[X]$ is said to be *solvable by radicals* over K if there exists a radical extension L of K containing the splitting field N of P.

COMMENTARY. – All of the elements of L can be written using radicals, but L can contain N strictly. We require that all of the roots of P lie in L; in the case of a polynomial irreducible over K, we can show that it is equivalent to require that one root of P lie in L (see, for example, the book by J.-P. Tignol, p. 345 and following).

OUTLINE OF THIS CHAPTER. – We will show in §12.2 that *if $P(X)$ is a polynomial of $K[X]$ which is solvable by radicals over K, with splitting field N over K, then* Gal$(N|K)$ *is a solvable group.* For this, we first need to construct a suitable radical extension of K (following §12.1). We will then show the converse of this fundamental result, in §12.4.

12.1.3 First Construction

Let us start from a radical extension L of K, containing N, defined by a radical tower $T = (K_i)_{0\leq i\leq r}$ with notation as in §12.1.1. Let us define the tower $T' = (K'_i)_{0\leq i\leq r+1}$ by $K'_0 = K, K'_1 = K[\zeta]$ where ζ is a primitive n-th root of unity, and $n = \operatorname{lcm}\{n_i; 1 \leq i \leq r\}$, $K'_{i+1} = K[\zeta, a_1, \ldots, a_i]$ for $1 \leq i \leq r$.

In this situation, K'_{i+1} is, by §10.2, a normal extension of K'_i for $i = 0, \ldots, r$, but we do not know if $L' = K'_{r+1}$ is a normal extension of K. For example, the radical tower $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\sqrt[4]{2}]$ is not in this case. Let us show that we can define a tower T'' that also satisfies this last property.

12.1.4 Second Construction

Let P_i be the minimal polynomial of a_i over K for $i = 1, \ldots, r$, and let A_i be the set of conjugates in $\mathbb{C}$ of a_i over K. The extension $L'' = K[\zeta, A_1, \ldots, A_r]$ is a normal extension of K, since it is the splitting field of $(X^n - 1)\prod_{1\leq i\leq r} P_i$.

Let us show that it is a radical extension of K of the same form as T'. It suffices to show that for every i with $1 \leq i \leq r$, and every $a \in A_i$, we have $a^{n_i} \in K\Big[\zeta\,,\, \cup_{j<i} A_j\Big]$.

Because a is conjugate to a_i over K, there exists a K-homomorphism $\sigma : K[a_i] \to \mathbb{C}$ such that $\sigma(a_i) = a$ and we can extend σ to a K-homomorphism

$\sigma' : K\Big[\zeta\,,\,\cup_{j\leq i}A_j\Big] \to \mathbb{C}$ such that $\sigma'(a_i) = a$. Since $K\Big[\zeta\,,\,\cup_{j<i}A_j\Big]$ is a normal extension of K (because it is the splitting field of $(X^n - 1)\prod_{1\leq j<i} P_j$) and $(a_i)^{n_i}$ belongs to it, the same holds for a^{n_i} which is conjugate to it, since $a^{n_i} = (\sigma'(a_i))^{n_i} = \sigma'((a_i)^{n_i})$.

Note that we can refine the tower $\Big(K\Big[\zeta\,,\,\cup_{j\leq i}A_j\Big]\Big)_{1\leq i\leq r}$ in such a way that the successive extensions are abelian (this is the case for $K[\zeta]$ over K, by §9.5) or cyclic (this is the case for extensions by each conjugate of a_i, by §10.2).

12.2 If a Polynomial Is Solvable by Radicals, Its Galois Group Is Solvable

THEOREM. – *Let K be a field contained in $\mathbb{C}$, and let P be a polynomial in $K[X]$ with splitting field N. If P is solvable by radicals, then* $\mathrm{Gal}(N|K)$ *is a solvable group.*

PROOF. – We just saw that there exists a radical extension L of K containing N, defined by a tower $(K_i)_{0\leq i\leq s}$ such that $K_0 = K$, $K_1 = K[\zeta]$ is an abelian extension of K, and $K_{i+1} = K_i[x_i]$ is a cyclic extension of K_i for $1 \leq i \leq s-1$, with $(x_i)^{n_i} \in K_i$, ζ a primitive n-th root of unity, $n = \mathrm{lcm}\,\{n_i; 1 \leq i \leq s-1\}$ and $L = K_s$ a normal extension of K.

Set $G_i = \mathrm{Gal}(L|K_i)$. The sequence $(G_i)_{0\leq i\leq s}$ satisfies the properties of §11.1. Indeed, condition 1) is clear; by §8.5 3), G_{i+1} is a normal subgroup of G_i, and as $G_i/G_{i+1} \simeq \mathrm{Gal}(K_{i+1}|K_i)$ is abelian, conditions 2) and 3) of §11.1 are satisfied. $\mathrm{Gal}(L|K)$ is thus a solvable group. By §11.4, the same holds for the group $\mathrm{Gal}(N|K)$, which is a quotient of $\mathrm{Gal}(L|K)$ by §8.4. ◊

12.3 Example of a Polynomial Not Solvable by Radicals

PROPOSITION. – *The polynomial $P(X) = X^5 - 10X + 5 \in \mathbb{Z}[X]$ is not solvable by radicals.*

PROOF. – By the preceding theorem, it suffices to determine its Galois group and show that it is not a solvable group. Let N denote the splitting field of P in $\mathbb{C}$, and set $G = \mathrm{Gal}(N|\mathbb{Q})$. P is an irreducible polynomial by Eisenstein's criterion. It has three real roots and two complex conjugate roots, which we call a and b; this can easily be determined by studying the sign of the derivative of P.

Complex conjugation on $\mathbb{C}$ induces an element of G that exchanges a and b and fixes the three other roots of P. Because $|G| = [N : \mathbb{Q}] = [N : \mathbb{Q}[a]][\mathbb{Q}[a] : \mathbb{Q}]$, the group G has order a multiple of 5, which by Cauchy's theorem (see Exercise 8.2) implies the existence of an element σ of order 5 in G. The group G is then identified with a subgroup of S_5 that contains a 5-cycle and a transposition. Thus, we have $G \simeq S_5$ (see Exercise 11.1.2) e)). As we know that S_5 is not solvable by Theorem 11.6.1, we can apply Theorem 12.2. $\diamondsuit$

12.4 The Converse of the Fundamental Criterion

PROPOSITION. – *Let $K \subset \mathbb{C}$ be a field, and let P be a polynomial in $K[X]$ with splitting field N over K and Galois group $G = \mathrm{Gal}(N|K)$. Assume that K contains a primitive n-th root of unity ζ with $n = [N : K] = |G|$. If G is a solvable group, then P is solvable by radicals.*

PROOF. – By §11.5, there exists a finite decreasing sequence $(G_i)_{0 \leq i \leq r}$ of subgroups of G such that

1) $G_0 = G \supset \ldots \supset G_r = \{e\}$;

2) G_{i+1} is a normal subgroup of G_i for $0 \leq i \leq r-1$;

3) G_i/G_{i+1} is cyclic of prime order p_i for $0 \leq i \leq r-1$.

Set $K_i = I(G_i)$ for $0 \leq i \leq r$; we have $K_0 = K$, and by §8.4, we also have $\mathrm{Gal}(K_{i+1}|K_i) \simeq \mathrm{Gal}(N|K_i)/\mathrm{Gal}(N|K_{i+1}) \simeq G_i/G_{i+1}$ for $0 \leq i \leq r-1$. Thus, $\mathrm{Gal}(K_{i+1}|K_i))$ is cyclic of prime order, and by §10.5, there exists an element $a_i \in K_{i+1}$ such that $(a_i)^{p_i} \in K_i$ and $K_{i+1} = K_i[a_i]$. This concludes the proof. $\diamondsuit$

12.5 The General Equation of Degree n

12.5.1 Algebraically Independent Elements

DEFINITION. – Let K be a field, and let L be an extension of K. Let $x_1, \ldots, x_n \in L$; these elements are said to be *algebraically independent over K* if the following homomorphism is injective: we define $f : K[X_1, \ldots, X_n] \to L$ by taking $f|K$ to be the inclusion of K into L, and setting $f(X_i) = x_i$ for $i = 1, \ldots, n$. In other words, $x_1, \ldots, x_n$ are algebraically independent if there exists no non-zero polynomial $P \in K[X_1, \ldots, X_n]$ such that $P(x_1, \ldots, x_n) = 0$.

12.5.2 Existence of Algebraically Independent Elements

PROPOSITION. – *For every integer n, there exist n algebraically independent complex numbers over $\mathbb{Q}$.*

PROOF. – Let us start with $\mathbb{Q}$, the field of rational numbers. It forms a countable set; its algebraic closure (see §14.1) $C(\mathbb{Q})$ inside $\mathbb{C}$ is also countable (check this); so its complement is non-empty. Choose an element x_1 in the complement. The extension of $C(\mathbb{Q})$ by x_1 is again countable; its algebraic closure $C(C(\mathbb{Q})(x_1))$ inside $\mathbb{C}$ is again countable, so again its complement is non-empty; choose an element x_2 in this complement. Continuing in this way, we obtain any number of algebraically independent elements. We can even choose the x_i to be real. ◇

12.5.3 The General Equation of Degree n

Let $x_1, \ldots, x_n$ be algebraically independent elements over $\mathbb{Q}$, and let $N = \mathbb{Q}(x_1, \ldots, x_n)$ be the field generated by these elements over $\mathbb{Q}$. Let P be the monic polynomial defined by

$$P(X) = \prod_{1 \leq i \leq n} (X - x_i).$$

The equation $P(X) = 0$ is called the *general equation of degree n over* $\mathbb{Q}$. Set

$$P(X) = X^n + \sum_{0 \leq k \leq n-1} a_k X^k \qquad \text{and} \qquad K = \mathbb{Q}(a_0, \ldots, a_{n-1}).$$

12.5.4 The Galois Group of the General Equation of Degree n

PROPOSITION. – *1) The Galois group* $\mathrm{Gal}(N|K)$ *of the general equation of degree n is isomorphic to S_n.*

2) The general equation of degree n is not solvable by radicals for $n \geq 5$.

PROOF. – 1) Every permutation $s \in \{1, \ldots, n\}$ induces a $\mathbb{Q}$-automorphism σ of N defined by $\sigma(x_i) = x_{s(i)}$ for $1 \leq i \leq n$; thus, we can consider S_n as a group of $\mathbb{Q}$-automorphisms of N. Set $L = I(S_n)$. Emil Artin's theorem shows that $[N : L] = n!$. Furthermore, as $a_k \in L$ for $0 \leq k \leq n$, by §3.2.2, we see that $K \subset L$. Finally, as N is the splitting field of P over K, we have $[N : K] \leq n!$.

We obtain $L = K$, so

$$\mathrm{Gal}(N|K) = \mathrm{Gal}(N|L) \simeq S_n.$$

2) It suffices to apply Theorem 12.2. ◇

COMMENTARY. – Figure 12.1 shows the beginning, written in an astonishingly modern style, of Abel's first memoir on the impossibility of resolving the general equation of degree five. He quickly extended this result to the general equation of arbitrary degree greater than or equal to five (in 1826). These results correspond to part 2) of Proposition 12.5.4. This impossibility had actually already been proved, in 1799, by Ruffini, but his enormously long proof had not convinced his colleagues, even after several modifications and simplifications.

MÉMOIRE SUR LES ÉQUATIONS ALGÉBRIQUES, OU L'ON DÉMONTRE L'IMPOSSIBILITÉ DE LA RÉSOLUTION DE L'ÉQUATION GÉNÉRALE DU CINQUIÈME DEGRÉ.

Brochure imprimée chez Grøndahl, Christiania 1824.

Les géomètres se sont beaucoup occupés de la résolution générale des équations algébriques, et plusieurs d'entre eux ont cherché à en prouver l'impossibilité; mais si je ne me trompe pas, on n'y a pas réussi jusqu'à présent. J'ose donc espérer que les géomètres recevront avec bienveillance ce mémoire qui a pour but de remplir cette lacune dans la théorie des équations algébriques.

Soit

$$y^5 - ay^4 + by^3 - cy^2 + dy - e = 0$$

l'équation générale du cinquième degré, et supposons qu'elle soit résoluble algébriquement, c'est-à-dire qu'on puisse exprimer y par une fonction des quantités a, b, c, d et e, formée par des radicaux.

FIGURE 12.1. The beginning of Abel's first memoir

Exercises for Chapter 12

Exercise 12.1. Examples of polynomials not solvable by radicals over $\mathbb{Q}$

1) Show that the following polynomials are not solvable by radicals over $\mathbb{Q}$.

- **a)** $X^5 - 14X + 7$;
- **b)** $X^5 - 7X^2 + 7$;
- **c)** $X^7 - 10X^5 + 15X + 5$.

2) Let P be an irreducible polynomial of $\mathbb{Q}[X]$ of prime degree $p \leq 5$. Assume that P has exactly two non-real roots. Show that P is not solvable by radicals.

Exercise 12.2. Cubic radical extensions

1) Let K be a field contained in $\mathbb{C}$, and let $P(X) = X^3 + pX + q$ be an irreducible polynomial in $K[X]$. Let x be a root of P, and let $D = d^2 = -4p^3 - 27q^2$ be the discriminant of P. Take an element $u = a + bx + cx^2$ of $K[x]$ with not lying in K, of minimal polynomial $X^3 + a'X^2 + b'X + c'$ over K.

   a) Determine a' and b' in terms of a, b, c, p, q.

   b) Show that $K[x]$ is a radical extension of K if and only if $-3D$ is a square in K.

   c) Extend the condition of part b) to the case where x is a root of an arbitrary irreducible polynomial $P(X) = X^3 + aX^2 + bX + c \in K[X]$.

2) Is the extension $\mathbb{Q}[\cos(2\pi/7)]$ of $\mathbb{Q}$ radical?

3) Let X_1, X_2, X_3 be indeterminates, and let s_1, s_2, s_3 be the elementary symmetric polynomials in these indeterminates.

   a) Show that $\mathbb{Q}(X_1, X_2, X_3)$ is not a radical extension of $\mathbb{Q}(s_1, s_2, s_3)$.

   b) Show that $\mathbb{Q}[j](X_1, X_2, X_3)$ is a radical extension of $\mathbb{Q}(s_1, s_2, s_3)$.

Exercise 12.3. A result of Galois

In this problem, we will make use of the results on transitive and solvable subgroups of S_p given in Exercise 11.4.

1) Let K be a field contained in $\mathbb{C}$, P an irreducible polynomial of prime degree $p \geq 5$ in $K[X]$, E the set of roots of P in $\mathbb{C}$, and N the splitting field of P over K.

   a) Assume that P is solvable by radicals. Show that $N = K[x, y]$ for every pair of distinct elements x and $y \in E$.

   b) Show the converse.

2) Let $K \subset \mathbb{R}$. Deduce from the above that a polynomial in $K[X]$, of prime degree greater than or equal to five and having exactly two real roots, is not solvable by radicals.

Exercise 12.4. Irreducible cubic equations: the necessity for non-reals

Consider the polynomial $P(X) = X^3 + pX + q$ with p and q real. Set $K = \mathbb{Q}(p, q)$, let a, b, and c denote the roots of P, and let $D = -4p^3 - 27q^2$ be its discriminant. Assume that P is irreducible over K and that $D > 0$, and let d be a real number such that $d^2 = D$.

In this case, the equation $P(x) = 0$ has three real roots; however, Cardan's formulas involve a square root of a negative number, i.e. a non-real number (see Exercise 2.4). Let us show that this cannot be otherwise. In order to show it, we first assume the contrary.

Suppose there exists a radical tower defined by a sequence $u_1, \ldots, u_n$ of strictly positive real numbers and a sequence $p_1, \ldots, p_n$ of prime numbers such that for $1 \leq i \leq n$, $(u_i)^{p_i} \in K[\sqrt[p_1]{u_1}, \ldots, \sqrt[p_{i-1}]{u_{i-1}}]$ and $a \in L = K[\sqrt[p_1]{u_1}, \ldots, \sqrt[p_n]{u_n}]$.

1) Show that $K[a, b, c] \subset L[d]$.

Define the sequence of fields $K_0 = K$, $K_1 = K[d], \ldots, K_{i+1} = K[d, \sqrt[p_1]{u_1}, \ldots, \sqrt[p_i]{u_i}]$ for $1 \leq i \leq n$, and let r be the smallest index i such that i such that $a \in K_{i+1}$.

2) Show that $r > 0$.

3) Show that $K[a, b, c] \subset K_{r+1}$ and that P is irreducible over K_r.

4) Show that $p_r = 3$, and then that K_{r+1} is a normal extension of K_r.

5) Deduce a contradiction.

COMMENTARY. – Otto Hölder was the first to clarify the problem posed by Cardan's formulas in 1891.

Solutions to Some of the Exercises

Solution to Exercise 12.1.

1) Use the arguments of §12.3 in the three cases.

2) The Galois group G of P contains the $\mathbb{Q}$-homomorphism induced by complex conjugation, and because P is irreducible, $|G|$ is a multiple of p. Identifying G with a subgroup Γ of S_p, we see that Γ contains a transposition and an element of order p, i.e. a p-cycle. Consequently, $\Gamma = S_p$ (see part **2)** of Exercise 11.1) and $G \simeq S_p$. Now we can conclude, using §12.2 and §11.6.

Solution to Exercise 12.2.

1) a) As u does not lie in K, it is of degree 3 over K. If x, y, z denote the roots of $X^3 + pX + q$ in $\mathbb{C}$, then the conjugates of u over K are u, $v = a + by + cy^2$, $w = a + bz + cz^2$, and the coefficients of the polynomial $(X - u)(X - v)(X - w)$ lie in K.

Using computations on symmetric polynomials, we find

$$\begin{aligned} a' &= -(u + v + w) = -3a + 2pc, \\ b' &= uv + vw + wu = 3a^2 + pb^2 - 4pac + p^2c^2 + 3qbc. \end{aligned}$$

b) In order for $K[x]$ to be a radical extension of K, it is necessary and sufficient that there exist an element $u = a + bx + cx^2 \in K[x]$ such that $K[x] = K[u]$, $u^3 \in K$, i.e. such that b or $c \neq 0$ and $a' = b' = 0$. As $a' = 0$ if and only if $a = 2pc/3$, these conditions are equivalent to $-(p^2c^2/3) + b^2p + 3bcq = 0$. This equation has a non-zero solution (b, c) in K^2 if and only if the discriminant of $pX^2 + 3qX - (p^2/3)$ is a square in K, which gives the result. Note that u is not unique.

c) By a variable change of the form $Y = X + \alpha$, we transform P into a polynomial of the form $X^3 + pX + q$ with the same discriminant D as P; we then recover the preceding conditions.

2) The minimal polynomial of $2\cos(2\pi/7)$ is given by $X^3 + X^2 - 2X - 1$ (see Exercise 2.6), which becomes $Y^3 - (7/3)Y - (7/27)$ after setting $Y = X + 1/3$. Its discriminant is $D = 49$. We deduce that $\mathbb{Q}[\cos(2\pi/7)]$ is a non-radical extension of $\mathbb{Q}$.

3) a) Set $d = (X_1 - X_2)(X_2 - X_3)(X_3 - X_1)$ and $D = d^2$. We know that the Galois group $\mathrm{Gal}(\mathbb{Q}(X_1, X_2, X_3)|\mathbb{Q}(s_1, s_2, s_3))$ is isomorphic to S_3, so the intermediate extensions are $\mathbb{Q}(s_1, s_2, s_3)[d]$ and $\mathbb{Q}(s_1, s_2, s_3)[X_i]$ for $i = 1, 2, 3$. As the quadratic extensions are radical, we still need to examine the case of extensions of degree 3. The extension $\mathbb{Q}(X_1, X_2, X_3)$ of $\mathbb{Q}(s_1, s_2, s_3)[d]$ is not radical since $-3D$ is not a square in $\mathbb{Q}(s_1, s_2, s_3)[d]$ (indeed, $D = d^2$ is a square and -3 is not a square). Let us now show that the extension $\mathbb{Q}(s_1, s_2, s_3)[X_i]$ of $\mathbb{Q}(s_1, s_2, s_3)$ is not radical either. If it were, $-3D$ would be a square in $\mathbb{Q}(s_1, s_2, s_3)$, so D would be a square in $\mathbb{C}(s_1, s_2, s_3)$, and we would have

$$\mathbb{C}(s_1, s_2, s_3)[X_i] = \mathbb{C}(s_1, s_2, s_3)[X_i, d] = \mathbb{C}(X_1, X_2, X_3),$$

which is false.

b) In this case, -3 is a square, which gives the conclusion.

Solution to Exercise 12.3.

The proof of course uses the Galois correspondence. We need to translate the property in the text into a condition on the Galois group $G = \mathrm{Gal}(N|K)$, or rather on the isomorphic subgroup of S_p obtained starting from an indexation of the roots as in §8.1.4. If we take a bijection $\varphi : \{1,\dots,p\} \to E$ with $x_i = \varphi(i)$, we obtain an injective group homomorphism $\Phi : G \to S_p$ such that $s = \Phi(\sigma)$ is the permutation given by $\sigma(x_i) = x_{s(i)}$.

1) a) If P is solvable by radicals, we know that $\Phi(G)$ is conjugate to a subgroup H of $\mathrm{GA}(p)$. Now, an element of $\mathrm{GA}(p)$ that has two fixed points is the identity. Consequently, an element of G which fixes two roots is the identity; in other words, $\mathrm{Gal}(N|K[x,y]) = \{\mathrm{id}\}$ for every pair of distinct elements x and $y \in E$. Thus $N = K[x,y]$.

b) We know that $\Phi(G)$ is transitive and the fact that $N = K[x,y]$ for every pair of distinct elements x and $y \in E$ is equivalent to the condition in $\Phi(G)$ that a permutation that fixes two elements of $\{1,\dots,p\}$ is the identity, hence the result (see Exercise 11.4).

2) If a and b denote the two real roots of P, then we cannot have $N = K[a,b]$ (with notation as above), since $K[a,b] \subset \mathbb{R}$ and $N \not\subset \mathbb{R}$. The result then follows from the first question.

COMMENTARY. – The result of this exercise is due to Galois, who stated it as follows: "For an equation of prime degree, which has no commensurable divisors, to be solvable by radicals, it is NECESSARY and SUFFICIENT that all the roots be rational functions of any two of them."

Solution to Exercise 12.4.

1) We know that $K[a,d] = K[a,b,c]$. As $K \subset L$ and $a \in L$, we have $K[a,d] \subset L[d]$, hence $K[a,b,c] \subset L[d]$.

2) $r = 0$ means that $a \in K_1 = K[d]$; this is impossible since a is of degree 3 over K and d is of degree 2 over K.

3) As a and d lie in K_{r+1}, we have $K[a,b,c] \subset K_{r+1}$ by **1)**.

Because K_r contains d, if it contains a root of P, then by **1)**, it must contain them all. But this contradicts the definition of r. Thus, P has no roots in K_r; as it is of degree 3, this suffices to show that it is irreducible over K_r.

4) As $K_{r+1} \supset K_r[a,b,c]$ and $K_r[a,b,c]$ is of degree 3 over K_r, we have $p_r = 3$ and $K_{r+1} = K_r[a,b,c]$. K_{r+1} is a normal extension of K_r.

5) Set $u = u_r$. Because K_{r+1} is a normal extension of K_r, and it contains one root of $X^3 - u$, it must contain the other roots, namely $j\sqrt[3]{u}$ and $j^2\sqrt[3]{u}$. But this contradicts $K_{r+1} \subset \mathbb{R}$.

13

The Life of Évariste Galois

The life of Évariste Galois is the most famous, fascinating, and commented life of any mathematician. It has even become something of a myth, like the lives of the immortal poets Rimbaud, Byron, or Keats.

Our knowledge of Galois' life contains enough gaps to allow imagination (and historians of science) to flourish. The books by Bourgne and Azra listed in the bibliography denounce some dangerous hypotheses and outright errors; see also their edition of Galois' complete works, containing portraits, reproductions of his writing, and all of his extant articles.

Évariste Galois was born on October 25, 1811, in Bourg-la-Reine, a town (renamed Bourg-l'Égalité during the Revolution!) located about 10 km south of Paris. His father, Nicolas Gabriel Galois, was a political liberal and the mayor of the commune during the Hundred Days; his strong personality assured him re-election under the Restoration. Apart from acting as mayor, he was also the director of a school. Galois' mother, Adélaïde Marie Demante, was the daughter of a magistrate. She appears to have played an important role in the education of her young son, particularly in the domain of Latin culture.

At the age of 12, Évariste entered the royal school of Louis-le-Grand. He was a brilliant student, but his teachers also commented that he had "somewhat bizarre manners" and was "rebellious"... (is this really extraordinary?) In October 1826, he entered the advanced rhetoric class, but at the beginning of the second trimester, he was demoted to the previous year because of his mediocre performance. At that time, all study was heavily based on classical culture, and sciences were studied only as extra work; this actually represented a regression with respect to the Napoleonic and

Revolutionary periods, during which mathematics teaching played a fundamental role in education.

Galois discovered mathematics thanks to his demotion, because he was allowed to take the extra courses. Alone, he read the whole of Legendre's *Elements of geometry* and Lagrange's texts on the resolution of equations, as well as works by Euler, Gauss, and Jacobi. In 1827, he obtained first prize in a national mathematics competition (the Concours Général, which still exists today); the following year, he obtained an accessit (awarded to the best papers after the first, second, and third prizes) in the same competition, as well as two successive accessits in Greek.

In 1828, he attempted the entrance examination for the Ecole Polytechnique, but failed, and remained at Louis-le-Grand, in the advanced mathematics class. His teacher, Monsieur Richard, was 33 years old; he soon came to deeply admire the genius he perceived in his student. He kept all of Galois' homework, and later gave them to another student of his, Charles Hermite. He encouraged Galois to publish his first research results; an article appeared on April 1, 1829, in the *Annales de mathématiques*, the journal founded by Joseph Gergonne.

It was at this point that difficulties and dramatic events began to accumulate around Galois. An article he sent to the Academy of Sciences was delivered to Cauchy and lost (Cauchy had already lost an article by Abel).

On July 2, Galois' father Nicolas committed suicide, unable to endure the attacks of the curé of Bourg-la-Reine, who among other things wrote a series of anonymous letters that he attributed to no other than Nicolas Galois! His funeral was the scene of a small riot.

A few days later, Galois once again attempted the entrance examination for the École Polytechnique. It was catastrophic; to the stupefaction of his professor, Galois failed. One of the examiners, either Dinet or Lefébure de Fourcy (probably Dinet), asked a question about logarithms which Galois found too simple or even stupid; it is said that he flung the blackboard eraser in the examiner's face. The mathematician Joseph Bertrand (born in 1822) denies this incident, but mentions the "crazy laughter of the gentlemen of the jury examining the candidates to the École Polytechnique (who do not, to my surprise, each occupy a chair at the Academy of Sciences, because their place is certainly not in posterity)."

Following the advice of his professor, Galois entered the École Normale. At that time, this school was known as the École Préparatoire, and was considered to be on a much lower level than the École Polytechnique. While there, he wrote the results of his research and presented them for the Grand Prize in Mathematics of the Academy of Sciences. Fourier (the Fourier of Fourier series, the theory of heat, the expedition to Egypt, etc.) took Galois' manuscript home with him, but died shortly afterward. The manuscript is now lost, but part of the results contained in it appeared in the *Bulletin des sciences mathématiques* published by the Baron de Férussac, in April

and June 1830. In the end, the Grand Prize was awarded to Abel (who had died the previous year) and Jacobi.

Galois' political opinions appear to have evolved very rapidly, and from that point on, he began to live a political life as intense as his mathematical one. During the famous days of July 27, 28, and 29, 1830, he and the other students were locked into their school to prevent them from participating in the action outside, while the students at the École Polytechnique battled on the barricades and made history. By October 1830, at the beginning of the academic year, Galois had turned into an active, ardent, and intrepid Republican, ready to defend the "rights of the masses", according to one member of his family. He joined the Society of Friends of the People on November 10 and openly criticized the opportunism of the director of the École Normale and the philosopher Victor Cousin, who from faithful followers of Charles X had become faithful followers of Louis-Philippe. He mingled criticism of their teaching with his political criticism and found himself indefinitely suspended.

The last mathematical article published in Galois' lifetime appeared on December 1. On December 5, he apparently authored a long letter published in the *Gazette des Écoles*, signed "a student at the École Normale", in which the director is derided in the following terms: "Everything in him announces the narrowest ideas and the most absolute routine." In early January, Galois was expelled by an exceptional decision of the board.

On January 2, 1831, a letter appeared (once again in the *Gazette des Écoles*), entitled *On the teaching of the sciences*, subtitled *Professors. Books. Examiners.* In the letter, Galois denounced the mediocrity of the teaching available to students: "When will students be given time to meditate on the mass of acquired knowledge.... Why do the examiners ask questions in a twisted way? It would seem that they are afraid to be understood by those who are being examined..... Do they fear that science is too easy?"

With no income, Galois opened a public course on higher algebra, on January 13, at the Caillot bookstore, 5 rue de la Sorbonne. The course probably did not last long. The advertisement, which appeared in the *Gazette des Écoles*, ran as follows: "This course will take place every Thursday at 1:15; it is aimed at young people who, feeling the incompleteness of algebra as taught in the colleges, wish to study the subject more deeply. The course will consist of theories, some of which are new, and none of which has ever been lectured on in public. We mention here a new theory of imaginaries, the theory of equations solvable by radicals, the theory of numbers and elliptic functions treated by pure algebra." Thirty people attended the first lecture.

The academician Denis Poisson advised Galois to write a new version of the memoir that had been presented a year earlier to Fourier and lost. On January 17, the Academy gave Poisson the task of reading the new manuscript, together with Sylvestre Lacroix. On March 16, Galois wrote to the academicians, pressing them to read his manuscript. Meanwhile,

political tensions ran high, as Louis-Philippe had managed to maneuver the Republicans out of power (in December 1830, he dissolved the National Guard, of which Galois was a member).

On May 9, 1831, after the acquittal of some young Republicans on trial, Galosi attended a banquet in the salon of the restaurant *Aux Vendanges de Bourgogne*; Alexandre Dumas and François-Vincent Raspail were also present. During the banquet, Galois proposed an unplanned toast. "To Louis-Philippe!" he said, raising his glass in one hand – "the fumes of the wine had removed my reason," he later explained – and a knife in the other. Those who did not see the knife protested, and during the following moments of effervescence, Alexandre Dumas became frightened and fled. The next day, Galois was arrested at his mother's home, and sent to the Sainte-Pélagie prison (near the Jardin des Plantes), to be judged on June 15.

The full text of the trial still exists. Galois' testimony reads: "Here are the facts. I had a knife which I had been using to cut food during the meal. I raised the knife, while saying *To Louis-Philippe, if he betrays.* The last words were heard only by my nearest neighbors, because of the whistles excited by the first part of my toast." The jury was indulgent, and Galois was acquitted.

An anonymous article published in the journal *Le Globe* mentions Galois' mathematical genius. On July 4, Poisson and Lacroix finally published their report on Galois' memoir, writing "We have made every effort to understand Galois' proof. His reasoning is neither sufficiently clear nor sufficiently developed to allow us to judge of its correctness... We can wait until the author has published his entire work in order to form a definitive opinion." They conclude that, for the moment, "we cannot propose approval of this memoir."

Galois was disappointed. But Poisson and Lacroix were not entirely mistaken; the text is extremely difficult to understand, and the author could certainly have provided additional explanations.

On July 14, Galois was arrested on the Pont-Neuf, at the head of a large group of demonstrators. He was again sent to Sainte-Pélagie, and this time condemned, on October 23, to six months of prison because he was not a first offender. His friend Ernest Duchatelet, who was arrested together with him, was condemned to just three months.

Galois continued to work in prison, where he also socialized with people like Nerval and Raspail.

In December, he submitted a new effort for publication. But the preface he wrote for his article was so polemical that the complete text ended up being published only in 1948, by René Taton. Bitter over the loss of his manuscripts and Poisson's lack of understanding, he violently attacked politicians and scientists, placing them on the same level: "If I had to address some words to the great men of this world or the great men of science... I swear that it would not be thanks." In the second part, he analyzes the

procedures he used to construct his theory, emphasizing that computations, even very elegant ones, *have their limits*, as do algebraic transformations *to such a point that in order to do them, they must have been foreseen.* He adds: "Jumping into the computations, grouping the operations, classifying them according to their difficulties and not according to their form: this, according to me, is the mission of future geometers [mathematicians]; this is the road I have followed in this article." To conclude, he emphasizes what he was unable to understand, and dreams of a time in which *egoism will no longer reign in the sciences*, and "people will study together, instead of sending sealed letters to the Academy; people will hasten to publish even their smallest observations, if they are new, and will not hesitate to add 'I do not know the rest.' "

Because of the cholera epidemic of early 1832, Galois was transferred on March 16 to a pension or sanatorium run by a certain Faultrier, near the Place d'Italie, along the Bièvre River, not far from the Croulebarbe Mill. At the time, this was located in the commune of Gentilly; later, it became part of the 13th arrondissement of Paris. In theory, Galois was scheduled to be set free on June 1, but it seems certain that he left prison earlier. In May 1832, he had a brief love affair with a young woman, Stéphanie D., whose true identity is still under discussion. He broke it off on May 14, and this appears to have been the cause of the duel he fought a few days later. The night before the duel, on May 29, Évariste assembled his latest discoveries in a splendid letter, addressed to a faithful friend, Auguste Chevalier. It is a dramatic scene to imagine. Foreseeing his death, pressed by time, he wrote this letter containing a summary of his mathematical work, in desperate urgency.

> Paris, May 29, 1832
>
> My dear friend,
>
> I have done several new things in analysis.
>
> Some of these things concern the theory of equations, others concern integral functions.
>
> In the theory of equations, I looked for conditions for the equations to be solvable by radicals....

He recalls the set of results that he obtained, concluding seven pages later with an obscure sketch of some notions later created by Riemann (many-sheeted Riemann surfaces are referred to as "the theory of ambiguity").

> My main meditations for some time now have been directed towards the application of the theory of ambiguity to transcendental analysis... But I do not have time now and my ideas on this immense terrain are not yet well developed...
>
> You will publicly request Jacobi or Gauss to give their opinions, not on the truth but on the importance of these theorems.

> After that, I hope there will be people who find profit in attempting to decipher this mess.

Rereading or wishing to modify one statement, he wrote in the margin: "There is something to be completed in this proof. I have no time."

He wrote other short letters, for example: "I am dying, the victim of an infamous coquette, and two fools of this coquette. My life is extinguished in a miserable cancan. Oh ! why die for so little.... Adieu ! I had a lot of life for the public good."

The exact circumstances of the whole adventure are not known, nor is the name of his adversary. In the morning of the May 30, Galois, grievously wounded and abandoned after the duel, was picked up by a peasant and carried to the Cochin hospital where he died of peritonitis on May 31, in the arms of his young brother Alfred, saying "Don't cry, I need all my courage to die at twenty." He was buried in the mass grave of the Montparnasse cemetery.

Accounts of his death appeared in a few newspapers, but they gave contradictory details. His friends organized a demonstration, which they postponed on hearing of the death of General Lamarque; it took place on June 5 and led to the massacre of the Saint-Merri cloister. Victor Hugo recounts the event in the chapter *The epic of the rue Saint-Denis* of his book *Les Misérables.*

Thanks to the devotion of Auguste Chevalier and his brother, the papers of Évariste Galois were collected, and his letter-testament was published in September 1832. It did not, however, attract any attention, even though it was published by Auguste Chevalier together with a presentation of the life of his friend ("A second condemnation threw him behind bars for six more months. Death awaited him at the exit"), to which Nerval added, in 1841: "He was killed in a duel the day after he was given his freedom." The romantic myth surrounding Galois was born from these lovely writings.

In 1835, Lacroix mentioned, in a note near the end of the sixth edition of his *Complements of elements of algebra* Galois' memoir, which he had read together with Poisson, saying:

> In 1828, Abel wrote to Legendre: "I have been happy enough to find a sure rule for recognizing if a given equation is by radicals or not. A corollary of my theory shows that generally, it is impossible to resolve equations superior to the fourth degree." (*Journal de Crelle*, year 1830, 1st cahier, p. 73.) This discovery was announced by Legendre to the Academy of Sciences on February 23, 1829; but Abel did not publish anything on the subject, and nothing to do with it was found in his papers....
>
> In 1831, a young Frenchman, Évariste Gallois (sic), who died the following year, announced, in a memoir presented to the Academy of Sciences, that 'for an irreducible equation of prime degree to be solvable by radicals, it is necessary and sufficient that given any two of its roots, the others can be deduced from them rationally', but his memoir

appeared practically unintelligible to the commissaries who examined it.

On September 4, 1843, Liouville announced to the Academy of Sciences that he just discovered, in the papers of Galois, a solution "as precise as it is deep" of the problem of the solvability of equations by radicals (*Comptes rendus hebdomadaires des séances de l'Académie des sciences*, vol. 17, pp. 448–449). Wishing, undoubtedly, to understand it better, he waited until October 1846 before publishing the texts by Galois, in his *Journal de mathématiques pures and appliquées*, with no commentary at all.

The truncated version of Galois' life presented by Liouville (who defended the institutions attacked by Galois, condemned his political activities, etc.) was the accepted version for 50 years, until a more precise version, based on forgotten and rediscovered documents, was published by Paul Dupuy in the *Annales de l'École Normale Supérieure.*

In the 1850s, the texts of Galois' memoirs finally became accessible to mathematicians. They initiated a great deal of work by Serret, Betti, Kronecker, Dedekind (who taught from them in Göttingen, in the winter of 1857–1858), Cayley, Hermite, Jordan (see his *Traité des substitutions* from 1870), etc. Their importance in the development of 20th century mathematics is immense.

Figure 13.1 is a reproduction of the portrait of Évariste Galois, drawn long after his death, from memory, by his brother Alfred, and published in *Le magasin pittoresque* in 1848.



FIGURE 13.1. Portrait of Évariste Galois by his brother Alfred, 1848

14
Finite Fields

In this chapter, we drop the assumption that the fields we consider are subfields of $\mathbb{C}$. We will make use of analogues of some of the definitions and results of previous chapters, which adapt to the case of finite fields; we do not always give the new proofs for these results. Note, however, that Theorem 14.1.3 proves the existence of an algebraic closure for each of the fields we will study; it plays a role analogous to that of $\mathbb{C}$ in the previous chapters. Fields of characteristic 2 are a particularly exciting subject of current research.

14.1 Algebraically Closed Fields

In this section, we consider arbitrary finite or infinite commutative fields of arbitrary characteristic (see §14.3).

14.1.1 Definition

A field C is said to be *algebraically closed* if every polynomial of degree greater than or equal to 1 in $C[X]$ factors into a product of linear factors or, equivalently, if every polynomial of degree greater than or equal to 1 in $C[X]$ has at least one root in C.

EXAMPLE. – The field $\mathbb{C}$ of complex numbers is an algebraically closed field, by d'Alembert's theorem (see Exercise 7.4).

14.1.2 Algebraic Closures

DEFINITION. – Let K be a field. An algebraic extension C of K which is algebraically closed is called an *algebraic closure* of K.

EXAMPLES. – 1) $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$.

2) $\mathbb{Q}$ has an algebraic closure that is a subfield of $\mathbb{C}$, namely the union of all algebraic extensions of finite degree of $\mathbb{Q}$ contained in $\mathbb{C}$.

14.1.3 Theorem (Steinitz, 1910)

Let K be a field.

1) *There exists an algebraic closure C of K. It is unique up to a non-unique K-isomorphism.*

2) *Let L be an algebraic extension of K, not necessarily contained in C, and let $\sigma : K \to C$ be a homomorphism. Then there exists an extension of σ to L.*

REMARK. – Note that a finite field K cannot be algebraically closed since the polynomial $1 + \prod_{a \in K} (X - a)$ has no roots in K.

PROOF. – Let us sketch a proof (see the book by A. and R. Douady listed in the bibliography for more details).

1) Let E be a set containing K, with sufficiently large cardinal. The algebraic extensions of K whose elements are in E form an ordered set, by extension, which is inductive. By Zorn's lemma, this set contains a maximal element C. Assuming that C is not algebraically closed leads to a contradiction. If K is finite, we can even avoid having recourse to Zorn's lemma, replacing it by a direct construction.

The isomorphism of two algebraic closures C and C' of K is a consequence of part 2), with L equal to C or C', noting that a K-homomorphism of an algebraic extension L (whether of finite or infinite degree) of a field K is an automorphism. This isomorphism is not unique.

2) Consider the set of pairs (L', σ'), where $K \subset L' \subset L$ and $\sigma' : L' \to C$ is an extension of σ; put an order on it by the extension relation. It is inductive, so we can use Zorn's lemma, which asserts that it has a maximal element (L_1, σ_1). We prove that $L_1 = L$ by assuming the contrary and obtaining a contradiction. ◇

COMMENTARY. – This theorem can be found in an article by Steinitz dating from 1910, which Bourbaki refers to as "having given birth to the current conception of algebra".

14.2 Examples of Finite Fields

1) The set $\mathbb{Z}/p\mathbb{Z}$, equipped with the natural addition and multiplication, is a finite field for every prime number p. From now on, we will denote this field by $\mathbb{F}_p$.

2) Let K be a finite field with q elements, and let P be an irreducible polynomial of degree n in $K[X]$ (such polynomials exist). Recall from §4.7 the construction of the extension $K[X]/(P)$ of K. A basis of this new field as a K-vector space is given by the set of classes of the powers X^k for $0 \leq k \leq n-1$; thus, it is finite-dimensional and has q^n elements.

   For example, if $K = \mathbb{Z}/2\mathbb{Z}$ and $P(X) = X^2+X+1$, then $K[X]/(P)$ has four elements, namely the classes of $0, 1, X, X+1$; let us denote them by $0, 1, x, x+1$. The multiplication law in K gives

$$\begin{aligned} x^2 &= -x-1 &&= x+1, \\ x^3 &= x(x+1) &&= x^2+x = 1, \\ (x+1)(x+1) &= x^2+1 &&= x, \quad x^4 = x, \quad \text{etc.} \end{aligned}$$

   In §14.5.1, we will show the existence and uniqueness, up to isomorphism, of a finite field with p^r elements for every prime number $p \geq 2$ and every integer $r \geq 1$.

14.3 The Characteristic of a Field

14.3.1 Definition

Let K be a field, and let $f : \mathbb{Z} \to K$ be the ring homomorphism defined by $f(1) = 1$. Then the image of f is a subring of K that is an integral domain, so its kernel is a prime ideal of $\mathbb{Z}$. The non-negative integer generating this ideal is called the *characteristic of* K, and written $\mathrm{char}(K)$.

EXAMPLES. – 1) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all fields of characteristic 0.

2) An example of a field having characteristic equal to a given prime number p is the field $\mathbb{F}_p$, a quotient of $\mathbb{F}_p[X]$ by an irreducible polynomial, or the (infinite) field of rational functions $\mathbb{F}_p(X)$.

14.3.2 Properties

A field of characteristic 0 contains a ring isomorphic to $\mathbb{Z}$, so it has a subfield isomorphic to $\mathbb{Q}$, whereas if $\ker(f) = (p)$ for some $p > 0$, then p must be prime and K contains a subfield isomorphic to $\mathbb{F}_p$. Thus, a field of characteristic 0 is infinite, and every finite field has non-zero prime characteristic. Every extension of a given field K has the same characteristic as K.

14.4 Properties of Finite Fields

14.4.1 Proposition

Let K be a finite field of characteristic $p > 0$ having q elements.

1) K is a finite-dimensional $\mathbb{F}_p$-vector space. If $r \geq 1$ is its dimension, then $q = p^r$.

2) The additive group of K is isomorphic to the group $(\mathbb{Z}/p\mathbb{Z}, +)^r$.

3) K^* is cyclic of order $q - 1 = p^r - 1$.

4) Every element $x \in K^*$ satisfies

$$x^{q-1} = 1,$$

and every element $x \in K$ satisfies

$$x^q = x.$$

COMMENTARY. – Part 3) gives the Primitive Element Theorem for finite fields; if L is a finite field extension of K, there exists an element x which generates the multiplicative group L^*, so $L = K[x]$.

PROOF. – 1) Because K is of characteristic p, K contains a subfield K' isomorphic to $\mathbb{F}_p$. We can then equip K with the structure of a finite-dimensional K'-vector space. If this dimension is r, the cardinal of K is p^r.

2) This follows from the vector space structure mentioned above.

3) Let us follow Gauss' original proof (pp. 53–54 of the *Recherches arithmétiques*). Let a be an element of maximal order $s \in K^*$. If $s = q - 1$, then a generates K^*, which is thus cyclic. Suppose $s < q - 1$. The set $E = \{a^k; 0 \leq k \leq s - 1\}$ has s elements, all roots of $X^s - 1$. Now, since a polynomial of degree s over a field has at most s roots, every element $b \in K^*$ not in E is not a root of $X^s - 1$. Thus, the order t of b does not divide s, and $\operatorname{lcm}(s, t) > s$. Let us write the decompositions of s and t as products of prime factors p_i, for $1 \leq i \leq r$, raised to positive or zero powers $s = \prod_{1 \leq i \leq r} p_i^{k_i}$ and $t = \prod_{1 \leq i \leq r} p_i^{l_i}$, and suppose the p_i are ordered in such a way that $k_i < l_i$ for $1 \leq i \leq j$ and $k_i \geq l_i$ otherwise. Set

$$u = \prod_{1 \leq i \leq j} p_i^{k_i}, \quad u' = \frac{s}{u}, \quad v = \prod_{1 \leq i \leq j} p_i^{l_i}, \quad \text{and} \quad v' = \frac{t}{v}.$$

As u' and v have no common prime factor, they are relatively prime. We see that a^u is of order u' and $b^{v'}$ is of order v. The element $a^u b^{v'}$ is of order $u'v = \operatorname{lcm}(s, t) > s$, which leads to a contradiction.

Unfortunately, there exists no algorithm for rapidly computing a generator of K^*, even in the case $K = \mathbb{F}_p$.

4) We know that in a finite group, the order of an element divides the order of the group. As K^* is of order $q-1$, we have $x^{q-1} = 1$ for every $x \in K^*$. Thus, for every $x \in K^*$, we have $x^q = x$; this property also holds for $x = 0$. Fermat's well-known "little theorem" is a special case of this statement. ◇

14.4.2 The Frobenius Homomorphism

PROPOSITION, DEFINITION. – *1) Let K be a (finite or infinite) field of characteristic $p > 0$. The map $F_p : K \to K$ defined by $F_p(x) = x^p$ is a (necessarily injective) field homomorphism, called the* Frobenius homomorphism *of the field. Thus, for every x and $y \in K$, we have*

$$(x+y)^p = x^p + y^p.$$

2) If L is an extension of a finite field K with q elements, the map $F_q : L \to L$ defined by $F_q(x) = x^q$ is a K-homomorphism called the Frobenius homomorphism of the extension.
3) If L is a finite extension of a finite field K with q elements, the Frobenius homomorphism F_q is a K-automorphism.

PROOF. – 1) Let k be such that $1 \leq k \leq p-1$. As $p! = k!(p-k)!\binom{p}{k}$, and furthermore the prime number p does not divide $k!(p-k)!$, it must divide $\binom{p}{k}$. The binomial formula then shows that $(x+y)^p = x^p + y^p$, so $F_p(x+y) = F_p(x) + F_p(y)$. The equality $F_p(xy) = F_p(x)F_p(y)$ is obvious.
2) If $\mathrm{char}(K) = p$, then F_q is a power of F_p and $x^q = x$ for x in K.
3) It suffices to note that F_q is a K-linear injective map between vector spaces of equal (finite) dimension. ◇

REMARK. – If K is a field of characteristic $p > 0$, the Frobenius homomorphism of K is the Frobenius homomorphism of the extension of $\mathbb{F}_p$ by K.

14.5 Existence and Uniqueness of a Finite Field with p^r Elements

14.5.1 Proposition

Let $p \geq 2$ be a prime and $r \geq 1$ an integer.
1) Let C be an algebraic closure of $\mathbb{F}_p$ (such a C exists by Steinitz' theorem 14.1.3). Then there exists a unique subfield K of C such that $|K| = q = p^r$.
2) K is the splitting field of the polynomials $X^q - X$ and $X^{q-1} - 1$.
3) Every field with p^r elements is isomorphic to K.

NOTATION. – We write $\mathbb{F}_q$ for the field with q elements.

PROOF. – 1) If such a field exists, its elements are roots of the polynomial $X^q - X$ in C. Let K be the set of these roots. K is stable under multiplication and taking inverses; it is also stable under addition, since if $F = F_p$ denotes the Frobenius homomorphism of C, we have $(x+y)^q = (x+y)^{p^r} = F^r(x+y) = F^r(x)+F^r(y) = x^q+y^q = x+y$. Thus, K is a subfield of C.

K has q elements because $P(X)$ decomposes into linear factors in C, and because it is prime to its derivative $P'(X) = -1$, it has only simple roots.

2) This follows from the construction of K.

3) Proposition 14.4.1 3) ensures the existence of a generator x of the multiplicative group K^*. Let $\varphi : \mathbb{F}_p[X] \to K$ be the surjective homomorphism defined by $\varphi(X) = x$, P the minimal polynomial of x over $\mathbb{F}_p$, and $\psi : \mathbb{F}_p[X]/(P) \to K$ the factorization of φ by the canonical projection $\pi : \mathbb{F}_p[X] \to \mathbb{F}_p[X]/(P)$. Then ψ is an isomorphism (Figure 14.1). As x is of order $q-1$, x is a root of the polynomial $X^{q-1}-1$, so P divides $X^{q-1}-1$. Set $X^{q-1} - 1 = P(X)S(X)$.

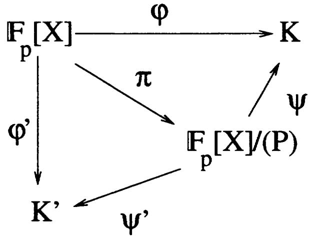


FIGURE 14.1.

Let K' be a field with p^r elements. The $q-1$ elements of K'^* are roots of $X^{q-1} - 1$. As P is not a constant, there exists at least one element $y \in K'^*$ which is a root of P. Let $\varphi' : \mathbb{F}_p[X] \to K'$ be the homomorphism defined by $\varphi'(X) = y$. As $\varphi'(P) = 0$, there exists $\psi' : \mathbb{F}_p[X]/(P) \to K'$ such that $\varphi' = \psi'\pi$. The map ψ' is an injective field homomorphism, so it is an isomorphism since $\mathbb{F}_p[X]/(P)$ and K' both have q elements. $\psi'\psi^{-1}$ is then an isomorphism of K onto K'. ◇

14.5.2 Corollary

For every irreducible polynomial P in $\mathbb{F}_p[X]$ of degree $r \geq 1$, $K = \mathbb{F}_p[X]/(P)$ is a field with $q = p^r$ elements, isomorphic to the subfield of the roots of $X^q - X$ in the algebraic closure C of $\mathbb{F}_p$.

PROOF. – The first assertion is proved using the arguments of §4.5.2, and the second follows from §14.5.1. ◇

14.6 Extensions of Finite Fields

PROPOSITION. – *Let K and L be two finite fields of characteristic p, and set $|K| = q = p^r$, $r \geq 1$.*

1) If L is an extension of K, there exists $s \geq 1$ such that $|L| = p^{sr} = q^s$. Every element of L is algebraic over K, of degree less than or equal to s.

2) If there exists $s \geq 1$ such that $|L| = p^{sr} = q^s$, then there exists a unique subfield of L isomorphic to K.

PROOF. – 1) $|L| = q^s$ is an immediate consequence of the finite-dimensional K-space structure s of L. If $x \in L$, then the family $\{x^k; 0 \leq k \leq n\}$ is not independent, which shows (as in §4.5.4) that x is algebraic over L.

2) Let C be an algebraic closure of L, and let K' be the subfield of C generated by the roots of $X^q - X$, as in §14.5.1. For every $x \in K'$, we have $x^q = x$, so we have $x^{q^s} = x$, which shows that $x \in L$. Thus, K' is isomorphic to K, by §14.5.1. ◇

EXAMPLE. – Thus, a field of order p^4 cannot lie inside a field of order p^6. However, each of these two fields contains a unique subfield of order p^2, and these two subfields are isomorphic.

14.7 Normality of a Finite Extension of Finite Fields

PROPOSITION. – *Let K be a finite field and L an extension of finite degree $s \in K$ with q^s elements. Then L is a splitting field of one of the polynomials $X^{q^s} - X$ and $X^{q^s-1} - 1$ over K, and thus it is a normal extension of K.*

PROOF. – If an irreducible polynomial in $K[X]$ has a root x in L, then it divides $X^{q^s} - X$, so it factors into linear factors in $L[X]$; moreover, its roots are simple. Thus, the conjugates of x over K lie in L. ◇

14.8 The Galois Group of a Finite Extension of a Finite Field

14.8.1 Proposition

Let K and L be two finite fields of characteristic p such that $K \subset L$. Suppose that $|K| = q = p^r$ and $|L| = q^s$ for integers r and $s \geq 1$. Then the Galois group $G = \mathrm{Gal}(L|K)$ is cyclic of order s, generated by $F = F_q$.

PROOF. – F is a K-automorphism of L, by Proposition 14.4.2 3). The powers of F are also K-automorphisms of L, so they are elements of G. Let us consider whether or not they are distinct.

We have $F^k(x) = x^{q^k}$ for every $x \in L$. In particular, $F^s = \text{id}(L)$. For $1 \leq k \leq s-1$, we have $F^k \neq \text{id}(L)$, otherwise every $x \in L^*$ is of order less than or equal to $q^k - 1$. Now, because L^* is a cyclic group, it has an element of order $q^s - 1$.

Thus, G has at least s elements, namely the K-automorphisms F^k for $0 \leq k \leq s-1$. So if x generates L, then its s images under the powers of F are distinct; these are the conjugates of x over K. As $[L : K] = s$, x cannot have any other conjugates, so G cannot have any other elements. Thus $|G| = s$, which gives the result. ◇

14.8.2 The Galois Correspondence

Let us keep the notation of the preceding proposition. The subgroups of the group G are all cyclic, generated by elements of the form F^k, where k divides s. The subfield of L invariant under F^k consists of the elements $x \in L$ such that $x^{q^k} = x$. For every k dividing s, L has a unique such subfield (cf. §14.5.1), so the Galois correspondence that we learned in Chapter 8 for subfields of $\mathbb{C}$ continues to hold for finite fields.

14.8.3 Example

Proposition 14.8.1 proves that $\text{Gal}(\mathbb{F}_{2^{12}}|\mathbb{F}_2) \simeq \mathbb{Z}/12\mathbb{Z}$.

For example, we have $I(\langle F^2 \rangle) \simeq \mathbb{F}_4$, $I(\langle F^6 \rangle) \simeq \mathbb{F}_{64}$, etc. The roots of unity different from 1 in $\mathbb{F}_{2^{12}}$ are the n-th roots for n dividing $4{,}095 = 5 \times 7 \times 9 \times 13$, i.e. $n = 5, 7, 9, 13, 35, 45, 63, 65, \ldots, 4{,}095$.

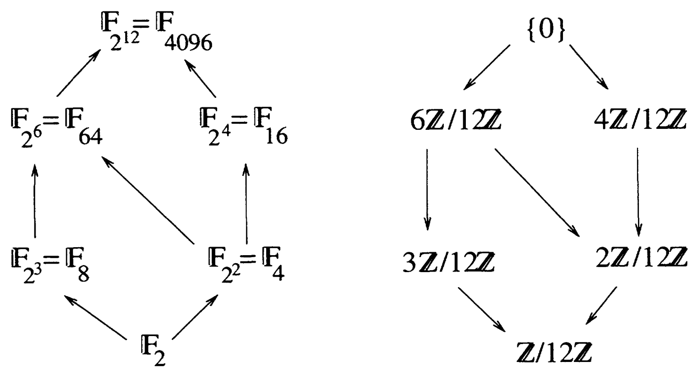


FIGURE 14.2. Galois correspondence for the extension $\mathbb{F}_{12}$ of $\mathbb{F}_2$

Exercises for Chapter 14

Exercise 14.1. The algebraic closure

1) Show that the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ is the union of the algebraic extensions of finite degree of $\mathbb{Q}$ contained in $\mathbb{C}$. Show that this closure is a countable set.

2) Let K be a field, L an algebraic extension of K, and C an algebraic closure of L. Show that C is an algebraic closure of K.

3) Let C be an algebraically closed field. What is the algebraic closure of C? What are the algebraic extensions of C? Give an example of an algebraically closed field C and a field L strictly containing C.

Exercise 14.2. Finite fields

1) Let K be a field and L a subfield of K. Show that K and L have the same characteristic.

2) Let K be a field. What is the intersection of the subfields of K?

3) Does there exist a field containing exactly 51 (resp. 129, 243, 1,024, 65,536, 65,537) elements?

4) Consider the polynomial $P(X) = X(X-1)^p$ in $\mathbb{F}_p[X]$. What is the multiplicity of 1 as a root of P? What about as a root of P'?

5) Set $K = \mathbb{F}_2(X)$. Show that the Frobenius homomorphism F of K is not an isomorphism of K.

Exercise 14.3. x generator, electronic transmission

Let p be a prime and $r \geq 1$ an integer.

1) Show that there exists an irreducible polynomial P of degree r in $\mathbb{F}_p[X]$ such that the multiplicative group K^* of the field K defined by $K = \mathbb{F}_p[X]/(P)$ is generated by the class $x \in X$ in K.

2) Assume that $p^r - 1$ is prime.

   a) What are the possible values of p?

   b) Show that for every irreducible polynomial P of degree r in $\mathbb{F}_p[X]$, the class $x \in X$ generates the multiplicative group K^* of the field $K = \mathbb{F}_p[X]/(P)$.

3) Show that the class $x \in X$ in $K = \mathbb{F}_2[X]/(X^4 + X^3 + X^2 + X + 1)$ does not generate K^*.

4) The goal of this question is to give a glimpse into the use of the field $K = \mathbb{F}_2[X]/(X^7 + X^3 + 1)$, isomorphic to $\mathbb{F}_{128}$, in the transmission of electronic messages. We follow an article by Pierre Arnoux published in the March 1988 issue of the magazine *Pour la Science.* The transmission is based on cyclic codes conceived in 1959–1960. A message to be transmitted is a sequence of 0's and 1's, and statistics show that transmission errors, i.e. reception of a 0 instead of a 1 or vice versa, are not very frequent; messages are cut into sections of 120 elements each.

a) Check that K is a field and that the class $x \in X$ in K generates K^*.

If we wish to transmit a sequence $a = (a_k)_{0 \le k \le 119}$ of elements of $\{0, 1\}$, we transmit the sequence $\varphi(a) = (a_k)_{0 \le k \le 126}$, where the last terms are defined by $x^7 \sum\limits_{0 \le k \le 119} a_k x^k = \sum\limits_{0 \le k \le 6} a_{120+k} x^k$.

b) Show that if $\varphi(a)$ is transmitted with an error, the message can nevertheless be reconstituted.

c) Show that if two messages are distinct, the sequences transmitted differ for at least three indices. What is the minimum number of errors that must be made to transmit a message incorrectly?

Exercise 14.4. $\alpha x^2 + \beta y^2 = -1$

Let K be a finite field of characteristic p with q elements, and let $f : K \to K$ be the map defined by $f(x) = x^2$.

1) a) Show that f is surjective if $p = 2$.

b) Show that the cardinal of the image of f is $(q + 1)/2$ if $p > 2$.

2) We want to show that given two non-zero elements α and β of a finite field K, there exist elements x and $y \in K$ such that $\alpha x^2 + \beta y^2 = -1$.

a) Show that such elements x and y exist if $p = 2$.

b) Assume $p > 2$. Determine the number of elements in the sets $\{1 + \alpha x^2; x \in K\}$ and $\{-\beta x^2; x \in K\}$. Deduce the existence of x and y.

Exercise 14.5. Zech's logarithm

1) Show that $K = \mathbb{F}_2[X]/(X^3 + X + 1)$ is a field.

2) Let x denote the class of X in K. Show that x generates K^*, and construct the table of powers of x in the basis $\{1, x, x^2\}$.

3) Define the function $Z : \{1, \ldots, 6\} \to \{1, \ldots, 6\}$ by $1 + x^i = x^{Z(i)}$. The function Z is called *Zech's logarithm.*

   a) Give the table of values of Z.

   b) Show that using Z, we can compute sums in K.

   c) Show that $Z(Z(i)) = i$.

COMMENTARY. – Zech's logarithm is an economical way to program the computation of addition in the field $\mathbb{F}_q$, but unfortunately, the place needed to stock the tables limits this procedure to small values of q.

Exercise 14.6. The field with 343 elements

1) Let a be an element of $\mathbb{F}_7$. For which values of a is the polynomial $X^3 - a$ irreducible in $\mathbb{F}_7[X]$? Deduce that $K = \mathbb{F}_7[X]/(X^3 - 2)$ is a field.

2) What are the possible orders of an element of the multiplicative group K^*? What is the order of the class $x \in X$ in K^*?

3) Find an element y of order 19 in K^*, of the form $a + bx$, with a and b in $\mathbb{F}_7$.

4) Use the above to find a generator u of the multiplicative group K^*. Determine the minimal polynomial of u over K.

Exercise 14.7. Sums of two squares

Let K be a finite field of characteristic p. In this problem, we propose to show that every element of K is a sum of the squares of two elements of K.

1) Prove a more precise result in the case $p = 2$.

   Now we assume $p > 2$.

2) Give an explicit formula in the case where -1 is a square in K.

3) Assume that -1 is not a square in K, and set $L = K[i]$ with $i^2 = -1$. Let $N : L \to K$ denote the norm map (whose value at x is equal to the product of the conjugates of x), and F the Frobenius homomorphism of L.

a) Determine the relation among $N(x)$, $F(x)$, and x; deduce an expression for $N(x)$ in terms of x.

b) Show that N induces a homomorphism from L^* to K^*. Determine its kernel. Conclude.

4) Express each of the elements of $\mathbb{F}_q$ as a sum of two squares for $q = 7, 13, 19$.

COMMENTARY. – The method we propose here is different from the one used in Exercise 14.4.

Exercise 14.8. Cyclotomic polynomials and finite fields

Let μ_k denote the group of k-th roots of unity in K.

Let K be a finite field of cardinal q, of characteristic p, and let C be an algebraic closure of K. Let $n \geq 1$ be an integer which is not a multiple of p (see part 1 of this problem for the case where n is a multiple of p). Let $\Phi = \Phi_n$ be the n-th cyclotomic polynomial in $\mathbb{Z}[X]$, and let $f : \mathbb{Z}[X] \to K[X]$ be the homomorphism defined by $f(1) = 1$ and $f(X) = X$. Let $\mu = \mu_n$, $L = K[\mu]$, $s = [L : K]$, and F the K-automorphism of L defined by $F(x) = x^q$. Finally, let G be the Galois group $\mathrm{Gal}(L|K)$.

1) In this question, we assume that n is a multiple of p, and we set $n = mp^r$ with $(m, p) = 1$ and $r > 0$. Show that $\mu = \mu_m$.

2) **a)** What is the cardinal of μ? What is the number of primitive roots in μ?

Set $\Phi_{d,K}(X) = \prod_{\zeta \in \mu_d, \zeta \text{ primitive}} (X - \zeta)$ for d dividing n.

b) Show that $f(X^n - 1) = \prod_{d \in D(n)} \Phi_{d,K}(X)$ in $K[X]$.

c) Deduce, using induction on n, that $f(\Phi_n(X)) = \Phi_{n,K}(X)$.

From now on, let Φ_n denote the polynomial $\Phi_{n,K}$ if no confusion is possible.

3) **a)** Show that s is the order of q in $U(n)$, by considering the $F^k(\zeta)$, where ζ is a generator of μ.

b) Deduce that the cyclotomic polynomial Φ_n factors into a product of irreducible polynomials of degree s in $K[X]$.

4) Assume $n = 8$, and set $\Phi = \Phi_8$, so $\Phi(X) = X^4 + 1$.

a) What happens to Φ if $p = 2$? Assume now that $p \neq 2$.

b) Show that Φ is reducible over $\mathbb{F}_q$ whatever the value of q. Note, however, that $X^4 + 1$ is irreducible in $\mathbb{Z}[X]$.

c) Determine L when $q = 5, 7, 17$, and factor Φ in $K[X]$ and in $L[X]$ as a product of irreducible factors.

5) Show that Φ_{12} is reducible in every finite field.

6) **a)** Give a necessary condition on n for Φ_n to be irreducible in $\mathbb{F}_q$.

b) Under what conditions on q is the polynomial Φ_n irreducible in $\mathbb{F}_q$ for $n = 3, 5, 14$?

Exercise 14.9. The field with 16 elements

1) What are the irreducible polynomials of degree 4 in $\mathbb{F}_2[X]$?

2) For each of the preceding polynomials P, let x denote the class of X in $\mathbb{F}_2[X]/(P)$. Construct the table of values of powers of x with respect to the basis $\{1, x, x^2, x^3\}$. Detail the case where x generates $\mathbb{F}_{16}^*$.

From now on, we set $P(X) = X^4 + X + 1$ and we define $\mathbb{F}_{16}$ as $\mathbb{F}_2[X]/(P)$. Recall (Exercise 9.6) that $\Phi_{15}(X) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$ in $\mathbb{Z}[X]$. We continue to write Φ_{15} for the polynomials in $\mathbb{F}_2[X]$ or $\mathbb{F}_{16}[X]$ obtained by reducing the coefficients modulo 2 or modulo 16.

3) **a)** Give a generator of the Galois group $\mathrm{Gal}(\mathbb{F}_{16}|\mathbb{F}_2)$.

b) Determine the factorization of Φ_{15} into a product of irreducible factors in $\mathbb{F}_2[X]$ (use the preceding exercise).

c) Give the roots of these factors in $\mathbb{F}_{16}[X]$ in terms of x.

Exercise 14.10. Roots of unity and "cosine"

1) Let p be a prime, $\mathbb{F}_q$ a field of characteristic p, C an algebraic closure of $\mathbb{F}_q$, k an integer prime to p, μ the group of k-th roots of unity in C, and ζ a generator of μ. Show that $c = \zeta + \zeta^{-1} \in \mathbb{F}_q$ if and only if $q = \pm 1 \bmod k$ (we distinguish the cases $\zeta \in \mathbb{F}_q$ and $\zeta \notin \mathbb{F}_q$).

2) Take $q = 16$ and $k = 17$.

   a) Determine the polynomial in $\mathbb{F}_2[X]$ whose roots are the distinct non-zero values $\omega + \omega^{-1}$ as ω runs through μ.

   b) Determine the possible values of c in terms of x for the field $\mathbb{F}_2[X]/(X^4 + X + 1)$ of exercise 14.9.

NOTE. – See the article by Mináč and Reis listed in the bibliography for further developments on this subject.

Exercise 14.11. Irreducibility of $X^p - X + a$

Let p be a prime, K a finite field of characteristic p, a an element of K, and $P(X) = X^p - X + a$. Let C be an algebraic closure of K.

1) Let x be a root of P in C. Determine the other roots of P in C.

2) Deduce that either the polynomial $X^p - X + a$ has all its roots in K, or it is irreducible in $K[X]$.

3) a) Let $a \neq 0$ in $\mathbb{F}_p$. Show that the splitting field of the polynomial $X^p - X + a$ over $\mathbb{F}_p$ is an extension of degree p of $\mathbb{F}_p$.

   b) Let n be an integer. Show that the polynomial $X^p - X + n$ is irreducible in $\mathbb{Q}[X]$ for an infinite number of values of n.

Exercise 14.12. Irreducible polynomials over a finite field

Let n and r be integers, and let p be a prime; set $q = p^r$. Let $I_q(n)$ denote the number of polynomials irreducible of degree n over $\mathbb{F}_q$.

1) Show that $I_q(n) \geq 1$, by considering a generator of an extension of degree n of $\mathbb{F}_q$.

2) Show that $q^n = \sum_{d \in D(n)} d I_q(d)$.

3) Deduce a formula giving $I_q(n)$.

4) Show that $X^{q^n} - X = \prod_{d \in D(n)} \prod_{P \in A(d)} P$, where $A(d)$ denotes the set of irreducible polynomials over $\mathbb{F}_q$ of degree d.

5) a) Show that $I_q(n) \simeq q^n/n$ in the neighborhood of $+\infty$.

b) Compute $I_q(n)$ in the cases $q = 2$, $1 \leq n \leq 9$, $q = 3$, $1 \leq n \leq 5$, $q = 5$, $1 \leq n \leq 3$, $q = 7$, $n = 1$ or 2.

Exercise 14.13. The quadratic reciprocity law

In this exercise, we assume that p is a prime number different from 2. We will use the same notation for an integer and for its class modulo p.

1) Let $f : U(p) \to U(p)$ be the homomorphism defined by $f(x) = x^2$, and set $A = \Im(f)$.

a) Let g be a generator of $U(p)$. Show that $x \in A$ if and only if x is an even power of g.

b) Deduce that $x \in A$ if and only if $x^{(p-1)/2} = 1$, and that $x \notin A$ if and only if $x^{(p-1)/2} = -1$.

c) Considering $\{-1, 1\}$ as a multiplicative group, check that setting $\varphi(x) = x^{(p-1)/2}$ gives a group homomorphism $\varphi : U(p) \to \{-1, 1\}$.

From now on, we set $\varphi(x) = \left(\frac{x}{p}\right)$; $\left(\frac{x}{p}\right)$ is called the *Legendre symbol* of x. The Legendre symbol extends to every integer $x \neq 0 \bmod p$.

2) Show that, for x and y in $U(p)$, we have

$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \qquad \left(\frac{1}{p}\right) = 1$$

$$\left(\frac{x^2}{p}\right) = 1 \qquad \left(\frac{x^{-1}}{p}\right) = \left(\frac{x}{p}\right)$$

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \qquad \sum_{x \in U(p)} \left(\frac{x}{p}\right) = 0.$$

3) Computation of $\left(\frac{2}{p}\right)$:

Let C be an algebraic closure of $\mathbb{F}_p$, and let ζ be a primitive eighth root of unity in C. Set $a = \zeta + \zeta^{-1}$.

a) Compute a^2.

b) Deduce the values of $\left(\frac{2}{p}\right)$ according to the values of p mod 8.

4) Main formula:

Let p and q be distinct primes: then $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$.

Let p and q be distinct odd primes, and let C be an algebraic closure of $\mathbb{F}_p$ and ζ a primitive q-th root of unity in C. Set $a = \sum_{k \in U(q)} \left(\frac{k}{q}\right) \zeta^k$; in this expression, k simultaneously denotes an element of $U(q)$ and the corresponding integer between 1 and $q-1$.

a) Show that

$$a^2 = (-1)^{(q-1)/2} \sum_{0 \le m \le q-1} \zeta^m \sum_{k \in U(q), k \neq m} \left(\frac{1 - mk^{-1}}{q}\right).$$

b) Show that

$$\sum_{k \in U(q), k \neq m} \left(\frac{1 - mk^{-1}}{q}\right) = -1 \qquad \text{for } 0 < m \le q-1,$$

$$\sum_{k \in U(q), k \neq m} \left(\frac{1 - mk^{-1}}{q}\right) = q-1 \qquad \text{for } m = 0.$$

c) Deduce that $a^2 = (-1)^{(q-1)/2} q$.

d) Show that $a^{p-1} = \left(\frac{p}{q}\right)$ (compute a^p).

e) Conclude.

5) Show that 30 is a square in $\mathbb{F}_{65{,}537}$ (note that $65{,}537 = 2^{2^4} + 1$ is a prime number).

COMMENTARY. – Special cases of the quadratic reciprocity law were indicated by Fermat, namely the values of $\left(\frac{\pm 2}{p}\right)$ and of $\left(\frac{\pm 3}{p}\right)$. They were

proved by Lagrange (1775) and Euler (1760) respectively. The general law was conjectured by Legendre (1785), who gave an incomplete proof of it; Gauss gave several proofs, the first one in 1801.

The quadratic reciprocity law relates the properties: "p is a quadratic residue modulo q " and " q is a quadratic residue modulo p ", which provides a rapid method for computing the Legendre symbol. The proof given above uses what are known as "Gauss sums". The ninth of Hilbert's famous 23 problems proposed in 1900 concerns generalizations of the quadratic reciprocity law for cubic residues, etc., which are currently objects of research.

Solutions to Some of the Exercises

Solution to Exercise 14.2.

1) The conditions $n \cdot 1 = 0$ in K and $n \cdot 1 = 0$ in L are equivalent.

2) The intersection of the subfields of K is the smallest subfield of K; it is $\mathbb{Q}$ if $\mathrm{char}(K) = 0$, $\mathbb{Z}/p\mathbb{Z}$ if $\mathrm{char}(K) = p$.

3) As the numbers 51 and 129 are not prime powers, there is no field with 51 or 129 elements.

To see that there exist fields of cardinal $243 = 3^5$, $343 = 7^3$, $1,024 = 2^{10}$, as well as $65,536$ which is prime ($65,536 = 2^{16}$ and $65,537$ is the Fermat number F_4), it suffices to note that they are all prime powers.

4) The multiplicity is the same in the two cases, namely p.

5) We know that F is injective. It is not surjective : for example, X is not in the image of F. Indeed, if $X = (P/Q)^2$, we would have $XQ^2 = P^2$, which is impossible since the first term is of odd degree and the second of even degree.

Solution to Exercise 14.3.

1) Let L be a field with p^r elements, y a generator of L^*, and P the minimal polynomial of y over $\mathbb{F}_p$. As $L = \mathbb{F}_p[y]$ is of degree r over $\mathbb{F}_p$, P is of degree r. Let $\pi : \mathbb{F}_p[X] \to K = \mathbb{F}_p[X]/(P)$ be the canonical projection. The ring homomorphism $f : \mathbb{F}_p[X] \to L$ defined by $f(X) = y$ induces an isomorphism $\varphi : K \to L$ and $x = \pi(X) = \varphi^{-1}(y)$ is a generator of K of minimal polynomial P over $\mathbb{F}_p$.

2) a) The primes of the form $2^r - 1$ are the Mersenne numbers, which are prime, for example, for $r = 2, 3, 5, 7$ but not for 11; the largest known Mersenne primes are for $r = 132,049$ (1983), $r = 216,091$ (1985), $r = 1,398,269$ (1996), etc. If $p \neq 2$, the condition that $p^r - 1$ is prime is equiv-

alent to $p = 3$ and $r = 1$, otherwise $p^r - 1$ is an even number greater than 2, so it cannot be prime.

b) Because the order of K^* is prime, it is generated by its non-trivial elements.

3) We have $x^5 - 1 = 0$ and $|K^*| = 15$.

4) a) The polynomial $X^7 + X^3 + 1$ is irreducible: to see this, it suffices to check that it is not divisible by an irreducible polynomial of degree less than or equal to 3. Furthermore, x generates K^* since 127 is prime.

b) Let $b = (b_k)_{0 \le k \le 126}$ be the sequence received. On reception, of the message, one computes the numbers c_k, $0 \le k \le 6$, defined by

$$x^7 \sum_{0 \le k \le 119} b_k \, x^k = \sum_{0 \le k \le 6} c_k \, x^k.$$

If the error concerns the l-th rank for $0 \le l \le 119$, we have

$$\begin{aligned} \sum_{0 \le k \le 6} c_k \, x^k + \sum_{0 \le k \le 6} b_{120+k} \, x^k &= x^7 \sum_{0 \le k \le 119} b_k \, x^k + x^7 \sum_{0 \le k \le 119} a_k \, x^k \\ &= x^{l+7}. \end{aligned}$$

If the error concerns the rank l, $120 \le l \le 126$, we have

$$\sum_{0 \le k \le 6} c_k \, x^k + \sum_{0 \le k \le 6} b_{120+k} \, x^k = x^{l-120}.$$

As x generates K^*, we can always find l, and if $0 \le l \le 119$, we can correct the received message.

c) We have $x^7 \sum_{0 \le k \le 119} a_k \, x^k + \sum_{0 \le k \le 6} a_{120+k} \, x^k = 0$ for every transmitted sequence $(a_k)_{0 \le k \le 126}$. If two transmitted sequences differed for a single index l with $0 \le l \le 126$, we would have $x^l = 0$; if they differed for two indices l and l', we would have $x^l = x^{l'}$. But this is impossible since x is of order 127 in K^*.

Three errors suffice: we can receive the sequence $a_0 = a_{120} = a_{123} = 1$, $a_k = 0$ otherwise, instead of the zero sequence, and we will not perceive the error, since

$$x^7 \sum_{0 \le k \le 119} a_k \, x^k + \sum_{0 \le k \le 6} a_{120+k} \, x^k = 0.$$

Solution to Exercise 14.4.

1) a) f is surjective since it is the Frobenius automorphism of K.

b) Let g be the restriction of f to K^*. It is a homomorphism of multiplicative groups. Its kernel has two elements: 1 and -1, which are distinct since $p > 2$. Thus, its image has $(q-1)/2$ elements (we can also see that if $x \neq 0$, then $x \neq -x$ since $p > 2$ and $x^2 = (-x)^2$, which enables us to count). The image of f also contains 0, which gives the result.

2) a) As α is non-zero, it is invertible. By **1) a)**, $-\alpha^{-1}$ is the square of an element x; we obtain the result by setting $y = 0$.

b) Because α and β are non-zero, the two sets have $(q+1)/2$ elements, as does the image of f. Thus their intersection is non-empty. Let z be an element of this intersection; there exists x and y in K such that $z = 1 + \alpha x^2 = -\beta y^2$, which gives the result.

Solution to Exercise 14.5.

1) The polynomial $X^3 + X^2 + 1$ has roots in $\mathbb{F}_2$, so it is irreducible over $\mathbb{F}_2$. The quotient $\mathbb{F}_2[X]/(X^3 + X^2 + 1)$ is an extension of degree 3 of $\mathbb{F}_2$, so it is a field with eight elements.

2) x generates K^*, which is of prime order. The table of powers of x, expressed in the basis $(1, x, x^2)$, is given in Table 14.1.

3) a) The values of Z are given in Table 14.2.

b) Because two elements are both powers of the generator x, their sum is computed by factoring out the smallest power of x. For $a < b$, we have $x^a + x^b = x^a(1 + x^{b-a}) = x^{a+Z(b-a)}$. For example, $x^3 + x^4 = x^3(1+x) = x^3x^5 = x^8 = x$.

c) $x^{Z(Z(i))} = 1 + x^{Z(i)} = 1 + 1 + x^i = x^i$, hence $Z(Z(i)) = i$.

Solution to Exercise 14.6.

1) We compute the cubes modulo 7 (Table 14.3).

$X^3 - a$ is irreducible in $\mathbb{F}_7[X]$ if a is not a cube modulo 7, i.e. if $a = 2, 3, 4, 5$.

2) K is a field with $7^3 = 343$ elements and K^* has $342 = 2 \times 9 \times 19$ elements. The order of an element of K^* is a divisor of 342. As $x^3 = 2$ and $2^3 = 8 = 1 \bmod 7$, x is of order 9.

	1	x	x^2
1	1		
x		1	
x^2			1
x^3	1		1
x^4	1	1	1
x^5	1	1	
x^6		1	1
x^7	1		

TABLE 14.1. Powers of x

i	1	2	3	4	5	6
Z	5	3	2	6	1	4

TABLE 14.2. Zech's logarithm

3) If $y = a+bx$ is of order 19, we have $y^{19} = 1$, so $y^{21} = y^2$. As $(a+bx)^7 = a + bx^7 = a + 4bx$, this gives

$$\begin{aligned} a^3 + 12a^2bx + 48ab^2x^2 + 64b^3x^3 &= a^2 + 2abx + b^2x^2, \\ a^3 + 5a^2bx - ab^2x^2 + 2b^3 &= a^2 + 2abx + b^2x^2; \end{aligned}$$

hence, $a^3 + 2b^3 = a^2, \quad 5a^2b = 2ab, \quad -ab^2 = b^2$.

We do not have $b = 0$ since y would lie in $\mathbb{F}_7$ and would not be of order 19. So we can simplify the last condition by b^2, which gives $a = -1$. The second condition is then satisfied, and the first implies that $b^3 = 1$, i.e. $b = 1, 2, 4$.

4) A generator of K^* is the product of three elements of order 2, 9, and 19 respectively; for example, $u = -xy = x - bx^2$. Let us compute the powers of u (Table 14.4). We immediately see that u is of degree 3 over $\mathbb{F}_7$ since it is a generator of K^*. As $u^3 = bu - 2$, $X^3 - bX + 2$ is the minimal polynomial of u over $\mathbb{F}_7$.

x	0	1	2	3	4	5	6
x^3	0	1	1	-1	1	-1	-1

TABLE 14.3.

	1	x	x^2
1	1	0	0
u	0	1	$-b$
u^2	$-4b$	$2b^2$	1
u^3	-2	b	$-b^2$

TABLE 14.4.

Solution to Exercise 14.7.

1) If $p = 2$, the Frobenius morphism F defined by $F(x) = x^2$ is an automorphism of K. Its surjectivity means that every number is a square in K.

2) If $-1 = b^2$, then because 2 is invertible, we have

$$a = \left(\frac{a+1}{2}\right)^2 + \left(b\frac{a-1}{2}\right)^2.$$

3) a) The Galois group of L over K has two elements, id and F. Hence,

$$N(x) = xF(x) = xx^q = x^{q+1}.$$

b) $N(xy) = N(x)N(y)$ is clear; $\ker(N) = \{x, x^{q+1} = 1\}$.

Let g be a generator of L^*; the elements of $\ker(N)$ are clearly the $g^{k(q-1)}$, $0 \leq k < q+1$. There are $q+1$ of them. Thus the image of N contains $(q^2-1)/(q+1) = q-1$ elements, so it is K^*. As an element of L can be written $u + iv$ with $u, v \in K$, for every $x \in K^*$, there exists u and v in K such that $N(u+iv) = x$, i.e. $u^2 + v^2 = x$.

4) If $q = 13$, then $q = 1 \bmod 4$, so -1 is a square; we see easily that $-1 = 5^2$, so $a = (6a+6)^2 + (4a-4)^2$.

If -1 is not a square, we can still work using successive tries. For example, the squares mod 19 are $1, 4, 9, -3, 6, -2, -8, 7, 5$, so $2 = 16+5 = 4^2+9^2$, $3 = 16+6 = 4^2+5^2$, etc.

Solution to Exercise 14.8.

1) It suffices to note that $X^n - 1 = (X^m - 1)^{p^r}$.

2) a) As $X^n - 1$ is prime to its derivative nX^{n-1} since n is not a multiple of p, it has n distinct roots and $|\mu| = n$. As μ is a cyclic subgroup of the cyclic group K^*, there are $\Phi(n)$ primitive n-th roots of unity.

b) The proof is the same as the one given in §9.4.2.

c) The property is obvious for $n = 1$. Let $n > 1$, and suppose that the property holds for every $k < n$. We have $X^n - 1 = \Phi_n(X) \prod_{d \in D(n), d \neq n} \Phi_d(X)$ in $\mathbb{Z}[X]$. Hence $f(X^n - 1) = f(\Phi_n(X)) \prod_{d \in D(n), d \neq n} f(\Phi_d(X))$, i.e. by the the induction hypothesis,

$$f(X^n - 1) = f(\Phi_n(X)) \prod_{d \in D(n), d \neq n} \Phi_{d,K}(X).$$

We conclude by comparing with the formula of **b)**.

3) a) We have $F(\zeta) = \zeta^q$ so, by induction, $F^k(\zeta) = \zeta^{q^k}$. As F is of order s in G, we see that $q^k \neq 1$ for $1 \leq k < s$ and $q^s = 1$. This gives the result.

b) As $K[\mu] = K[\zeta]$ for every generator ζ of μ, every root of Φ_n is of degree s over K. Thus, the irreducible factors of Φ_n, which are minimal polynomials of these generators, all have the same degree s.

4) a) Φ factors into linear factors: $\Phi(X) = (X + 1)^4$.

b) If $p \neq 2$, we have $q = 1$, 3, 5, 7 mod 8. As these elements are of order 1 or 2, we have $s = 1$ or 2; thus ζ is never of degree 4 over $\mathbb{F}_q$ and $X^4 + 1$ is reducible over $\mathbb{F}_q$ whatever the value of q.

c) The cases proposed here lead to different situations.

- $q = 5$. As 5 is of order 2 in $U(8)$, $X^4 + 1$ factors into a product of two irreducible factors of degree 2 in $\mathbb{F}_5[X]$. Noting that $-1 = 4$ mod 5, we have $X^4 + 1 = (X^2 - 2)(X^2 + 2)$ in $\mathbb{F}_5[X]$. If we set $2 = \alpha^2$ and $L = \mathbb{F}_5[\alpha]$, we have $X^4 + 1 = (X - \alpha)(X + \alpha)(X - 2\alpha)(X + 2\alpha)$.

- $q = 7$. Because 7 is of order 2 in $U(8)$, the degree of the irreducible factors is again 2. As -1 is not a square in $\mathbb{F}_7$, we will translate the equality of $\mathbb{R}[X] : X^4 + 1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$. We see that $2 = 3^2$ mod 7, so $X^4 + 1 = (X^2 - 3X + 1)(X^2 + 3X + 1)$. If we set $i^2 = -1$ and $L = \mathbb{F}_7[i]$, we obtain $X^4 + 1 = (X + 2 - 2i)(X + 2 + 2i)(X - 2 - 2i)(X - 2 + 2i)$.

- $q = 17$. As $17 = 1$ mod 8, $X^4 + 1$ factors into linear factors and

  $L = \mathbb{F}_{17} : X^4 + 1 = (X^2 - 4)(X^2 + 4) = (X - 2)(X + 2)(X - 8)(X + 8)$.

5) Distinguish the cases $p = 2$, $p = 3$, and $p \geq 5$, and use the same reasoning as in **3) b)**; as $U(12) \simeq (\mathbb{Z}/2\mathbb{Z})^2$, we see that $s = 1$ or 2.

6) a) The condition "Φ is irreducible over K" is equivalent to $s = \deg(\Phi) = \varphi(n)$, in other words to the fact that q generates $U(n)$. This means that $U(n)$ is cyclic, i.e. (see Exercise 9.8, 4 b)) that n is of the form $2p^k$ or p^k, for an odd prime p.

b) As q must generate $U(n)$, we find that

$$q = 2 \bmod 3 \quad \text{if} \quad n = 3; \quad q = 2, 3 \bmod 5 \quad \text{if} \quad n = 5;$$

$$q = 3, 5 \bmod 14 \quad \text{if} \quad n = 14.$$

Solution to Exercise 14.9.

1) A polynomial of degree 4 is reducible if it has a root or 2 irreducible factors of degree 2. We know that the only irreducible polynomial of degree 2 over $\mathbb{F}_2$ is $X^2 + X + 1$. Since the only reducible polynomial of degree 4 has no root over $\mathbb{F}_2$, it is $X^4 + X^2 + 1 = (X^2 + X + 1)^2$. Now, a polynomial of degree 4 over $\mathbb{F}_2$ which has no roots must be one of the four polynomials $X^4 + X + 1, X^4 + X^3 + 1, X^4 + X^3 + X^2 + X + 1$ and $X^4 + X^2 + 1$. The preceding remark shows that only the first three of these polynomials are irreducible.

2) Tables 14.5 and 14.5*bis* give the powers of x expressed in the basis 1, x, x^2, x^3 in each case. We see that x is a generator in the two first cases (to obtain this result alone, it would suffice to check that x is not of order 3 or 5, which is shown by the computation of x^3 and x^5) but not in the third.

	X^4+X+1				X^4+X^3+1			
k	1	x	x^2	x^3	1	x	x^2	x^3
0	1				1			
1		1				1		
2			1				1	
3				1				1
4	1	1			1			1
5		1	1		1	1		1
6			1	1	1	1	1	1
7	1	1		1	1	1	1	
8	1		1			1	1	1
9		1		1	1		1	
10	1	1	1			1		1
11		1	1	1	1		1	1
12	1	1	1	1	1	1		
13	1		1	1		1	1	
14	1			1			1	1
15	1				1			

TABLE 14.5.

1	x	x^2	x^3
1			
	1		
		1	
			1
1	1	1	1
1			

TABLE 14.5.*bis*

3) a) The Galois group $\mathrm{Gal}(\mathbb{F}_{16}|\mathbb{F}_2)$ is cyclic of order 4, generated by the Frobenius automorphism F, defined by $F(z) = z^2$.

b) Because x is a root of Φ_{15} having minimal polynomial X^4+X+1, we know that Φ_{15} is divisible by X^4+X+1. This shows that the irreducible factors of Φ_{15} in $\mathbb{F}_2[X]$ have degree 4 (see Exercise 14.8). Thus Φ_{15} is

a product of two irreducible factors over Φ_2, and the second one is the quotient $\Phi_{15}(X)/(X^4+X+1) = X^4+X^3+1$. Hence,

$$\Phi_{15}(X) = (X^4+X+1)(X^4+X^3+1).$$

c) The distinct roots of Φ_{15} are all the generators of the cyclic group $\mathbb{F}_{16}^*$, i.e. the x^k where k is prime to 15. Thus, we find that $\Phi_{15}(X)$ is equal to

$$(X-x)(X-x^2)(X-x^4)(X-x^7)(X-x^8)(X-x^{11})(X-x^{13})(X-x^{14}).$$

The conjugates of x over $\mathbb{F}_2$ are the images of x under the elements of the Galois group $\mathrm{Gal}(\mathbb{F}_{16}|\mathbb{F}_2)$; thus they are $x = \mathrm{id}(x), x^2 = F(x), x^4 = F^2(x)$, and $x^8 = F^3(x)$. These are the four roots of X^4+X+1.

The roots of X^4+X^3+1 are the other roots of $\Phi_{15} : x^7, x^{11}, x^{13}, x^{14}$. We can check that these are the conjugates of x^7, since $F(x^7) = x^{14}$, $F^2(x^7) = x^{13}$, and $F^3(x) = x^{11}$.

Solution to Exercise 14.10.

1) Let us first assume that $c \in \mathbb{F}_q$. If $\zeta \in \mathbb{F}_q$, we have $\zeta^{q-1} = \zeta^k = 1$, so $q-1 = 0 \bmod k$. If $\zeta \notin \mathbb{F}_q$, we have $c^q = c = \zeta + \zeta^{-1} = \zeta^q + \zeta^{-q}$, so $(\zeta^{q-1}-1)(\zeta - \zeta^{-q}) = 0$. As the first factor is non-zero, we have $\zeta = \zeta^{-q}$, so $\zeta^{q+1} = 1$ and $q+1 = 0 \bmod k$.

Now assume that $q = \pm 1 \bmod k$.

If $q = 1 \bmod k$, then $\zeta^{q-1} = 1$ shows that ζ lies in $\mathbb{F}_q$, so c does as well. If $q = -1 \bmod k$, then $\zeta^{q+1} = 1$ implies that $\zeta = \zeta^{-q}$, so $c^q = \zeta^q + \zeta^{-q} = \zeta^{-1} + \zeta = c$. Thus $c \in \mathbb{F}_q$.

2) a) The primitive 17th roots of unity are all distinct in an algebraic closure of $\mathbb{F}_{16}$, since $X^{17}-1$ is prime to its derivative. If $c = \omega + \omega^{-1}$, we have $\omega^2 = c\omega + 1$; if $c = 0$, then $\omega = 1$, otherwise c can take eight distinct values since if $\omega + \omega^{-1} = \eta + \eta^{-1}$, we have $(\omega - \eta)(\omega\eta - 1) = 0$, so $\eta = \omega$ or $\eta = \omega^{-1}$. We have $\omega^2 = c\omega + 1, \omega^4 = c^3\omega + c^2 + 1$, $\omega^8 = c^7\omega + c^6 + c^4 + 1$, $\omega^{16} = c^{15}\omega + c^{14} + c^{12} + c^8 + 1$, $\omega^{17} = c^{15} + \omega(c^{16} + c^{14} + c^{12} + c^8 + 1)$. As $\omega^{17} = 1 = c^{15}$, c is a root of the polynomial $Q(X) = X^8 + X^7 + X^6 + X^4 + 1$, whose roots are exactly the eight possible values of c.

b) We see that x is a root of Q. Let ζ be a 17th root of unity such that $x = \zeta + \zeta^{-1}$. As ζ generates the group of 17th roots of unity in $\mathbb{F}_16[\zeta] \simeq \mathbb{F}_{256}$, the possible non-zero values of c are the $\zeta^k + \zeta^{-k}$ with $k = 1, \ldots, 8$. Table 14.6 gives the result of the computations; the first line gives the value of k, and the second gives the expression for the quantity $\zeta^k + \zeta^{-k}$ in terms of x. We can also use the factorization $Q(X) = (X^4+X+1)(X^5-1)/(X-1)$.

1	2	3	4	5	6	7	8
x	x^2	$x+x^3$	$1+x$	x^2+x^3	x^3	$1+x+x^2+x^3$	$1+x^2$

TABLE 14.6.

Solution to Exercise 14.11.

1) For every $u \in \mathbb{F}_p$, we have $(x+u)^p-(x+u)+a = x^p+u-x-u+a = 0$. The p roots of P are thus the $x+u$ with $u \in \mathbb{F}_p$.

2) If P is reducible in K, there exist polynomials S, T in $K[X]$ such that $P(X) = S(X)T(X)$ with $\deg(S) = s$, $1 \leq s \leq p-1$. The roots of S are among the roots of P; they are of the form $x+u$, with u in $\mathbb{F}_p$. Their sum is of the form $sx+v$ with $v \in \mathbb{F}_p$; as it belongs to K (up to sign, it is a coefficient of S), we have $sx \in K$, so $x \in K$ since $s \neq 0$. Because one root of the polynomial P lies in K, they all do, by **1)**.

3) a) The polynomial $X^p - X + a$ has no root in $\mathbb{F}_p$, since $x^p - x = 0$ for every $x \in \mathbb{F}_p$. Thus, it is irreducible in $\mathbb{F}_p[X]$, which gives the result.

b) The preceding question shows that $X^p - X + n$ is irreducible in $\mathbb{F}_p[X]$, so it also is irreducible in $\mathbb{Z}[X]$ and in $\mathbb{Q}[X]$, whenever n is an integer not divisible by p.

Solution to Exercise 14.12.

1) Let C be an algebraic closure of $\mathbb{F}_q$, and let L be the subfield of C with q^n elements; it is an extension of degree n of $\mathbb{F}_q$. Let x denote a generator of L^*; x is of degree n over $\mathbb{F}_q$, so its minimal polynomial over $\mathbb{F}_q$, which is irreducible over $\mathbb{F}_q$, is of degree n, and consequently, $I_q(n) \geq 1$.

2) Let L be as above. Consider the equivalence relation: "x and y are equivalent if they have the same minimal polynomial over $\mathbb{F}_q$". If x is of degree d over $\mathbb{F}_q$, then x has d distinct conjugates over $\mathbb{F}_q$, and d divides n. The desired equality follows from the partition of L into equivalence classes.

3) The Möbius inversion formula gives $nI_q(n) = \sum\limits_{d \in D(n)} \mu(d) q^{n/d}$.

4) If P is an irreducible polynomial of degree d for some d dividing n, then every root of P is in an intermediate extension between $\mathbb{F}_q$ and $\mathbb{F}_{q^n}$, so it satisfies $x^{q^n} - x = 0$. This proves that P divides $X^{q^n} - X$. By **2)**, the sum of the degrees of such polynomials is equal to the degree of $X^{q^n} - X$, which concludes the proof.

5) a) We have $0 < 1 - (nI_q(n)/q^n) = \sum\limits_{d \in D(n), d \neq 1} \mu(d) q^{n(-1+1/d)} < nq^{-n/2}$.

b) The results are given in Table 14.7. Note the form of the equivalence of **a)**.

$q = 2$

n	1	2	3	4	5	6	7	8	9
q^n	2	4	8	16	32	64	128	256	512
$I_q(n)$	2	1	2	3	6	9	18	30	56

$q = 3$

n	1	2	3	4	5
q^n	3	9	27	81	243
$I_q(n)$	3	2	8	18	48

$q = 5$

n	1	2	3
q^n	5	25	125
$I_q(n)$	5	10	40

$q = 7$

n	1	2
q^n	7	49
$I_q(n)$	7	21

TABLE 14.7.

COMMENTARY. – These tables show that we can choose an irreducible polynomial of degree n over $\mathbb{F}_q$ in many ways. However, certain polynomials are more useful than others.

Solution to Exercise 14.13.

1) a) Every $x \in U(p)$ can be written as a power of g; the result follows since p is odd.

b) On the one hand, $g^{p-1} = 1$; on the other, if $a = g^{(p-1)/2}$, we have $a \neq 1$ and $a^2 = 1$. Thus, because $\mathbb{F}_p$ is a field, we have $a = -1$.

2) The properties follow from **1)**. The last one follows from the equality between the number of even powers and the number of odd powers of g in $U(p)$.

3) a) As $\zeta^4 = -1$, we have $\zeta^2 = -\zeta^{-2}$, so $a^2 = \zeta^2 + 2 + \zeta^{-2} = 2$.

b) We know that $\left(\frac{2}{p}\right) = 2^{(p-1)/2}$, so $\left(\frac{2}{p}\right) = a^{p-1} = a^p/a$. As $a^p = (\zeta + \zeta^{-1})^p = \zeta^p + \zeta^{-p}$, a^p depends on the values of p mod 8.

If $p = \pm 1$ mod 8, then $a^p = a$, so $\left(\frac{2}{p}\right) = a^{p-1} = 1$; 2 is a square modulo p.

If $p = \pm 5$ mod 8, as $\zeta^4 = -1$, $a^p = \zeta^5 + \zeta^{-5} = -a$, so $\left(\frac{2}{p}\right) = -1$; 2 is not a square modulo p.

4) a) Let k, l, m denote both an element of $\mathbb{F}_q$ and the corresponding integer between 0 and $q-1$. The multiplicativity of the Legendre symbol implies that

$$\begin{aligned} a^2 &= \sum_{k,l \in U(q)} \left(\frac{k}{q}\right)\left(\frac{l}{q}\right)\zeta^{k+l} = \sum_{0 \le m \le q-1} \zeta^m \sum_{k \in U(q), k \ne m} \left(\frac{k}{q}\right)\left(\frac{m-k}{q}\right) \\ &= (-1)^{(q-1)/2} \sum_{0 \le m \le q-1} \zeta^m \sum_{k \in U(q), k \ne m} \left(\frac{1 - mk^{-1}}{q}\right), \end{aligned}$$

since $\left(\frac{k}{q}\right)\left(\frac{m-k}{q}\right) = \left(\frac{-k^2}{q}\right)\left(\frac{1-mk^{-1}}{q}\right) = (-1)^{(q-1)/2}\left(\frac{1-mk^{-1}}{q}\right)$.

b) If $m = 0$, then $\sum_{k \in U(q), k \ne m} \left(\frac{1-mk^{-1}}{q}\right) = q - 1$. If $1 \le m \le q-1$, we have

$$\sum_{k \in U(q), k \ne m} \left(\frac{1-mk^{-1}}{q}\right) = \sum_{l \in U(q), l \ne 1} \left(\frac{l}{q}\right) = -1;$$

this follows because $\{1 - mk^{-1}; k \in U(q), k \ne m\} = \{l; l \in U(q), l \ne 1\}$ and from the last equality of **2)**.

c) We obtain $a^2 = (-1)^{(q-1)/2}\left(q - 1 - \sum_{1 \le m \le q-1} \zeta^m\right) = (-1)^{(q-1)/2} q$.

d) To begin with,

$$\begin{aligned} a^p &= \sum_{k \in U(q)} \left(\frac{k}{q}\right)\zeta^{kp} = \sum_{l \in U(q)} \left(\frac{lp^{-1}}{q}\right)\zeta^l \\ &= \left(\frac{p^{-1}}{q}\right)\sum_{l \in U(q)} \left(\frac{l}{q}\right)\zeta^l = \left(\frac{p}{q}\right) a. \end{aligned}$$

Furthermore, $a \ne 0$ by **c)**.

e) The preceding computations allow us to write

$$\left(\frac{q}{p}\right) = q^{\left(\frac{p-1}{2}\right)} = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} a^{p-1} = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} \left(\frac{p}{q}\right).$$

5) The number 65,537 is prime (see Exercise 14.2), and it suffices to show that $\left(\frac{30}{65,537}\right) = 1$.

By **3)**, $\left(\frac{2}{65,537}\right) = 1$ since $65,537 = 1 \bmod 8$.

By **4)**, we have

$$\left(\frac{3}{65,537}\right) = \left(\frac{65,537}{3}\right) = \left(\frac{2}{3}\right) = -1$$

and

$$\left(\frac{5}{65,537}\right) = \left(\frac{65,537}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

This gives the result. But it does not produce the numbers with square equal to 30 modulo 65,537. A formal computation program gives $\pm 27,\ 135$.

15
Separable Extensions

In this chapter, we consider arbitrary commutative fields, i.e. finite and infinite fields of arbitrary characteristic.

15.1 Separability

DEFINITION. – Let K be a field and L an extension of K. An element $a \in L$ that is algebraic over K is said to be *separable over* K if it is a simple root of its minimal polynomial.

An algebraic extension L of a field K is *separable* if every element of L is separable over K.

An irreducible polynomial in $K[X]$ that has no multiple roots in an algebraic closure of K is called *separable*; if it has multiple roots, it is called *inseparable.*

EXAMPLES. –

1) If $L \subset \mathbb{C}$ is an algebraic extension of a field K, then L is a separable extension of K (see §4.4.5).

2) Algebraic extensions of finite fields and of characteristic 0 fields are always separable, by Proposition 15.5 below.

COMMENTS. – The notion of separability dates back to Steinitz (1910). A non-separable algebraic element of degree n over a field K has less than n conjugates over K.

15.2 Example of an Inseparable Element

Let $\mathbb{F}_p(U)$ be the field of rational functions in U with coefficients in $\mathbb{F}_p$. Let K be the image of the Frobenius homomorphism $F: \mathbb{F}_p(U) \to \mathbb{F}_p(U)$ defined by $F(x) = x^p$ (Figure 15.1). Set $V = F(U) = U^p$. Then V belongs to K, and U is algebraic over K since it is a root of the polynomial $X^p - V \in K[X]$. However, we can easily check that it does not lie in K.

Let us show that the polynomial $X^p - V \in K[X]$ is irreducible over K. The proof is immediate for $p = 2$. In the general case, we have $X^p - V = F(X^p - U)$ and $F|\mathbb{F}_p(U)$ is an isomorphism, so it suffices to show that $X^p - U$ is irreducible in $\mathbb{F}_p(U)[X]$. But $\mathbb{F}_p[U]$ is a factorial ring, with fraction field $\mathbb{F}_p(U)$, in which U is an irreducible element, so it is prime and we can apply Eisenstein's criterion.

Thus U is of degree p over K, with minimal polynomial $X^p - V$. In $\mathbb{F}_p(U)[X]$, we have $X^p - V = X^p - U^p = (X - U)^p$. Thus, U is a unique root, of order p, of its minimal polynomial, so U is not separable over K.

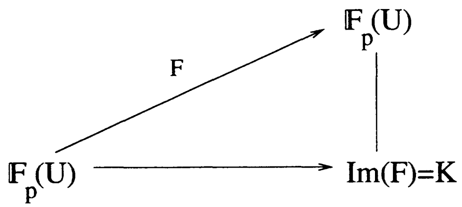


FIGURE 15.1.

15.3 A Criterion for Separability

PROPOSITION. – *Let p be a prime, K a field of characteristic p, L an extension of K, and a an element of L which is algebraic over K, of minimal polynomial P over K.*

1) *a is separable over K if and only if $P'(a) \neq 0$ or, equivalently, $P' \neq 0$. The conjugates of a over K are then also separable over K.*

2) *If a is not separable over K, then P is of the form*

$$P(X) = \sum_{0 \le k \le n} a_k X^{kp}.$$

PROOF. –

1) We have $P(X) = (X-a)S(X)$, so $P'(X) = S(X) + (X-a)S'(X)$. If a is separable over K, we know that $S(a) \neq 0$, so $P'(a)$ is non-zero. The converse is immediate. Finally, $P' \neq 0$ is equivalent to $P'(a) \neq 0$ since P is the minimal polynomial of a over K and P' cannot vanish at a if $P' \neq 0$.

2) We have $P' = 0$ by a), which implies that $P(X) = \sum_{0 \leq k \leq n} a_k X^{kp}$. ◊

15.4 Perfect Fields

Let K be a field of characteristic $p > 0$. Let K^p denote the image of the Frobenius homomorphism $F : K \to K$ defined by $F(x) = x^p$. As F is injective, it is a subfield of K.

A field is said to be *perfect* if it is of characteristic 0 or of characteristic $p \neq 0$ with the property that $K^p = K$.

EXAMPLE. – Every finite field is perfect.

15.5 Perfect Fields and Separable Extensions

PROPOSITION. – *A field K is perfect if and only if every algebraic extension of K is separable.*

PROOF. – Assume that K is perfect. The case $\mathrm{char}(K) = 0$ was considered in §4.4.5. Assume $p = \mathrm{char}(K) \neq 0$, and suppose that L is an algebraic extension of K, and a is an element of L, non-separable over K, of minimal polynomial P over K. By Proposition 15.3, $P(X) = \sum_{0 \leq k \leq n} a_k X^{kp}$ (with $a_n = 1$). As $K^p = K$, there exist elements $b_0, \ldots, b_n \in K$ such that $(b_k)^p = a_k$ for $0 \leq k \leq n$; hence, $P(X) = (\sum_{0 \leq k \leq n} b_k X^k)^p$. Thus, P is not irreducible over K, which contradicts the hypothesis.

Conversely, suppose that every algebraic extension of K is separable. If $\mathrm{char}(K) = 0$, then K is perfect by definition. Suppose $p = \mathrm{char}(K) \neq 0$; let us show that the Frobenius homomorphism F is surjective. Let $a \in K$, and let b denote a root of $X^p - a$ in an algebraically closed extension of K. Let S be the minimal polynomial of b over K. As $X^p - a = (X-b)^p$, S divides $(X-b)^p$, so it is of the form $(X-b)^s$. But as $K[b]$ is a separable extension of K, we have $s = 1$, so $b \in K$. ◊

15.6 Galois Extensions

15.6.1 Definition

An algebraic extension N of an arbitrary field K is said to be *Galois* if $K = I(\mathrm{Gal}(N|K))$, the field of invariants of $\mathrm{Gal}(N|K)$.

15.6.2 Proposition

An algebraic extension is Galois if and only if it is normal and separable.

COMMENTARY. – This proposition explains why we used the term Galois extensions for normal extensions in Chapter 8 (cf. §8.2). Indeed, as we saw in earlier chapters, the Galois extensions of a perfect field are exactly the normal extensions since all extensions of such a field are separable.

PROOF. – Let N be a Galois extension of K. Let $x \in N$ have minimal polynomial P over K, and let $x_1 = x, \dots, x_n$ be the distinct conjugates of x in N. The polynomial $S(X) = \prod_{1 \leq i \leq n} (X - x_i)$ is invariant under the elements of $\mathrm{Gal}(N|K)$, so its coefficients lie in $I(\mathrm{Gal}(N|K)) = K$. It follows that $P = S$ and the roots of P are all distinct and lie in N. The extension N of K is thus normal and separable.

Now, let N be a normal separable extension of K. We have the inclusion $K \subset I(\mathrm{Gal}(N|K))$. If $x \in N$ does not lie in K, then its minimal polynomial over K is of degree strictly greater than 1. As the extension is separable, there exists a conjugate y of x, different from x, in an algebraic closure C of N. There exists a K-homomorphism $\sigma : K[x] \to C$ such that $\sigma(x) = y$. We can extend σ to N; let σ' denote this extension. As N is a normal extension of K, σ' defines an element of $\mathrm{Gal}(N|K)$ such that $\sigma'(x) \neq x$; consequently, $x \notin I(\mathrm{Gal}(N|K))$. ◇

15.6.3 The Galois Correspondence

The main theorem of the Galois correspondence given in §8.5 extends to all Galois extensions of finite degree, using the same proof as the one given in §8.5.

Toward Chapter 16

It would be possible to develop the different aspects of Galois theory almost indefinitely; we choose to stop at this point and devote one final chapter to giving some idea of two domains of current research.

16

Recent Developments

16.1 The Inverse Problem of Galois Theory

16.1.1 The Problem

Is every finite group the Galois group of an extension of the field $\mathbb{Q}$? The answer to this question is not yet completely known.

The study of Galois groups of polynomials of degree 2, 3, and 4 enables us to assert that any subgroup of S_2, S_3, S_4 is the Galois group of an extension of $\mathbb{Q}$. We also gave examples of polynomials in $\mathbb{Q}[X]$ with Galois group S_p, $p \geq 5$ prime (see §12.3 and Exercise 12.1).

In 1981, Jean-Pierre Serre indicated that aside from abelian groups, the answer is actually known for very few groups; until now, however, it has been positive in every case. The groups A_n and S_n (Hilbert, 1892), solvable groups (a result whose proof is extremely difficult, due to Shafarevitch, 1954), the groups $\mathrm{PSL}(2, \mathbb{F}_p)$ for certain values of p... all have been shown to occur as Galois groups of extensions of $\mathbb{Q}$.

The situation has developed considerably over the last few years. In 1985, work by Belyi, Fried, Llorente, Matzat, Thompson, and others showed that 18 of the 26 simple groups known as the sporadic groups occur as Galois groups of extensions of the field $\mathbb{Q}$. Many other results have been proved since then (see the books by B. Matzat and J.-P. Serre listed in the bibliography).

16.1.2 The Abelian Case

PROPOSITION. – *Let G be a finite abelian group. Then there exists a finite Galois extension K of $\mathbb{Q}$ havivg Galois group isomorphic to G.*

PROOF. – We know that G is a finite product of cyclic groups: $G = \prod_{i\in I} \mathbb{Z}/n_i\mathbb{Z}$, where the n_i may or may not be distinct. For every $i \in I$, choose a prime p_i such that $p_i = 1 \bmod n_i$. By Lejeune–Dirichlet's theorem of arithmetic progressions (which states that if a and b are relatively prime, then the arithmetic progression $(an + b)_{n\in\mathbb{N}}$ contains an infinite number of primes) we can choose the p_i all distinct.

Set $N = \prod_{i\in I} p_i$ and $\zeta = e^{2i\pi/N}$. By §9.5, group $\mathrm{Gal}(\mathbb{Q}[\zeta]|\mathbb{Q})$ is isomorphic to the group $U(N)$ of invertible integers modulo N. By §9.1.2, $U(N) \simeq \prod_{i\in I} U(p_i) \simeq \prod_{i\in I} \mathbb{Z}/(p_i - 1)\mathbb{Z}$. Because $p_i - 1 = k_i n_i$, $U(N)$ has $H = \prod_{i\in I} n_i\mathbb{Z}/(p_i - 1)\mathbb{Z}$ as a subgroup. Writing H' for the corresponding subgroup of $\mathrm{Gal}(\mathbb{Q}[\zeta]|\mathbb{Q})$, $K = I(H')$ is a normal extension of $\mathbb{Q}$, since H' is a normal subgroup of G; its Galois group is $U(N)/H \simeq G$. ◊

16.1.3 Example

Let us consider the case where $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. We have $n_1 = n_2 = 3$, $n_3 = 5$; we can take $p_1 = 7$, $p_2 = 13$, $p_3 = 11$, which leads to $N = 1{,}001$.

We know that $U(N) \simeq U(7) \times U(13) \times U(11) \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$, and we set $H \simeq 3\mathbb{Z}/6\mathbb{Z} \times 3\mathbb{Z}/12\mathbb{Z} \times 5\mathbb{Z}/10\mathbb{Z}$.

16.2 Computation of Galois Groups over $\mathbb{Q}$ for Small-Degree Polynomials

The whole of this section concerns Galois groups over $\mathbb{Q}$. The first problem is to effectively compute the Galois group of a given polynomial in $\mathbb{Q}[X]$. The computations are actually more approachable than what Galois believed, thanks to computers; the search for algorithms to compute the Galois group of a polynomial has developed a great deal since the 1970s, using ideas that can be traced back to work of Lagrange from 1770. By 1995, algorithms to determine the Galois groups of all polynomials of degree less than or equal to 11 had been implemented. For higher degrees, Galois' remark remains valid: for polynomials of degree 15, for example, one is dealing with groups that are subgroups of S_{15}, a group having more

than 1.3×10^{12} elements. The following sections are based on an article by Richard Stauduhar, listed in the bibliography.

16.2.1 Simplification of the Problem

Let P be a polynomial of degree n of $\mathbb{Q}[X]$, and let N be the splitting field of P. To determine $\mathrm{Gal}(N|\mathbb{Q})$, we can:

1) Reduce to a polynomial having only simple roots. Indeed, we know that the polynomial $S = P/\gcd(P, P')$ has the same roots as P, but they are all simple roots: thus, its splitting field is still N, and its Galois group is the same as that of P.

2) Next, reduce to a polynomial having integral coefficients. It suffices to multiply P by the least common multiple of the denominators of the coefficients of P.

3) Finally, reduce to a monic polynomial with integral coefficients. To accomplish this, if $P(X) = \sum_{0\leq k\leq n} a_k X^k \in \mathbb{Z}[X]$, it suffices to consider the polynomial $P_1(Y) = Y^n + \sum_{0\leq k\leq n-1} a_k (a_n)^{n-k-1} Y^k$. As $P_1(a_n X) = (a_n)^{n-1} P(X)$, the polynomial P_1 has the same Galois group as P.

Because of this, we will assume from now on that P is a monic polynomial in $\mathbb{Z}[X]$.

16.2.2 The Irreducibility Problem

Recall that there exist algorithms to decompose any polynomial in $\mathbb{Z}[X]$ into a product of polynomials in $\mathbb{Z}[X]$, all of which are irreducible in $\mathbb{Q}[X]$. These algorithms apply to all polynomials of small degree which we consider here. The starting point of these methods is the article by Berlekamp on the factorization of polynomials with coefficients in a finite field (1967). If a polynomial is not irreducible, it is not always easy to find its Galois group in terms of the Galois groups of its irreducible factors. One can try to adapt the methods described below.

From now on, we assume that P is a monic irreducible polynomial in $\mathbb{Z}[X]$.

16.2.3 Embedding of G into S_n

Recall what we did in §8.1.4. If E denotes the set of roots of P in $\mathbb{C}$, then a bijection $\varphi : \{1, \ldots, n\} \to E$ defines an indexation of the roots of P,

$x_i = \varphi(i)$, giving an embedding $\Phi : G \to S_n$. Two bijections $\{1, \dots, n\} \to E$ define embeddings $G \to S_n$ whose images are conjugate subgroups of S_n. We will only identify the Galois group as a subgroup of S_n up to conjugation.

16.2.4 Looking for G Among the Transitive Subgroups of S_n

The group $\Phi(G)$ is a transitive subgroup of S_n (*cf.* §8.1.4); to know which one, we can undertake to make a list of all the transitive subgroups of S_n up to conjugation, and to find criteria for eliminating subgroups from the list one by one, until only one remains. Such criteria can be obtained by considering polynomial functions of the roots, the first examples of which were given by Lagrange. This procedure gives the structure of G without giving an explicit isomorphism from G to the corresponding subgroup of S_n.

In the remainder of this chapter, we will restrict ourselves to the case $n = 4$, except in §16.2.6, where we state a general result.

16.2.5 Transitive Subgroups of S_4

The list of transitive subgroups of S_4 is as follows:

1) Order 24: S_4;

2) Order 12: the alternating group A_4 whose elements are the identity, the eight 3-cycles, the three double transpositions;

3) Order 8: three subgroups isomorphic to the dihedral group D_4; these groups are mutually conjugate, since they are the 2-Sylow subgroups of S_4; the elements of these subgroups can be obtained by numbering the vertices of the square described in §8.7.2 in different ways via the bijections f, g, h (Table 16.1).

f	g	h
$A \to 1$	$A \to 1$	$A \to 1$
$B \to 2$	$B \to 2$	$B \to 3$
$C \to 3$	$C \to 4$	$C \to 2$
$D \to 4$	$D \to 3$	$D \to 4$

TABLE 16.1.

$$H_1 = \{\text{id}, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\},$$

$$H_2 = \{\text{id}, (13), (24), (12)(34), (13)(24), (14)(23), (1234), (1432)\},$$

$$H_3 = \{\text{id}, (14), (23), (12)(34), (13)(24), (14)(23), (1243), (1342)\}.$$

4) Order 4: $V = \{\text{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$, the Klein *Vierergruppe*;

5) Three mutually conjugate cyclic subgroups of the subgroups of order 8 of S_4, generated by 4-cycles:

   a) K_1 : id,$(1\ 3\ 2\ 4), (1\ 2)(3\ 4), (1\ 4\ 2\ 3)$,

   b) K_2 : id,$(1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)$,

   c) K_3 : id,$(1\ 2\ 4\ 3), (1\ 4)(2\ 3), (1\ 3\ 4\ 2)$.

Our results are shown (up to conjugation) in Figure 16.1.

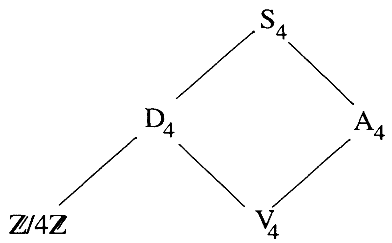


FIGURE 16.1.

16.2.6 Study of $\Phi(G) \subset A_n$

Set

$$D = \prod_{1 \le i < j \le n} (x_i - x_j)^2$$

and

$$d = \prod_{1 \le i < j \le n} (x_i - x_j)$$

(D is the discriminant of P). Let $T(X_1, \ldots, X_n) = \prod_{1 \le i < j \le n} (X_i - X_j)$, and let t be a transposition of S_n. We have $t(T) = -T$; we can assume that $t = (n-1\ \ n)$. In this case, the sign change comes from $t(X_{n-1} - X_n) = -(X_{n-1} - X_n)$. It follows that $s(T) = T$ if $s \in A_n$ and $s(T) = -T$ if $s \notin A_n$.

PROPOSITION. – *We have $\Phi(G) \subset A_n$ if and only if $d \in \mathbb{Z}$.*

PROOF. – Suppose $\Phi(G) \subset A_n$. For every $\sigma \in G$, we have $s = \Phi(\sigma) \in A_n$ so $\sigma(d) = s(T)(x_1, \ldots, x_n) = T(x_1, \ldots, x_n) = d$. Consequently, $d \in \mathbb{Q}$. If we write $d = p/q$ with $(p, q) = 1$, we know that $p^2/q^2 = D \in \mathbb{Z}$ since it is the resultant of a monic polynomial in $\mathbb{Z}[X]$, so $q = \pm 1$ and $d \in \mathbb{Z}$.

Suppose $\Phi(G) \not\subset A_n$. There exists σ in G such that $s = \Phi(\sigma) \notin A_n$, so $\sigma(d) = s(T)(x_1, \ldots, x_n) = (-T)(x_1, \ldots, x_n) = -d$. Hence $d \notin \mathbb{Z}$. ◇

The case $n = 3$. If $d \in \mathbb{Z}$, we have $G \simeq A_3 \simeq \mathbb{Z}/3\mathbb{Z}$. If $d \notin \mathbb{Z}$, we have $G \simeq S_3$.

The case $n = 4$. If $d \in \mathbb{Z}$, we can have $G \simeq A_4$ or $G \simeq V$. If $d \notin \mathbb{Z}$, we can have $G \simeq S_4$, $G \simeq D_4$ or $G \simeq \mathbb{Z}/4\mathbb{Z}$.

REMARK ON THE TEST $d \in \mathbb{Z}$. – This test comes down to seeking the integral roots of the polynomial

$$R(X) = X^2 - D = (X - d)(X + d),$$

known as the A_4-resolvent, a polynomial whose coefficients are known to be integral. We can compute D exactly, by successive divisions, and look to see if it is a square in $\mathbb{Z}$. We can also compute a good approximation (say on the order of 10^{-9}) of each of the roots, both real and complex, of P. This gives a good approximation Δ of D; then, knowing that D is an integer, we take D to be the nearest integer to the approximate value Δ.

16.2.7 Study of $\Phi(G) \subset D_4$

More precisely, the point is to determine if $\Phi(G)$ is contained in one of the three subgroups of S_4 isomorphic to D_4. Consider the polynomial $U(X_1, \ldots, X_4) = X_1X_2 + X_3X_4$ introduced by Lagrange (cf. §10.8). If $s \in S_4$, then $s(U)(X_1, \ldots, X_4)$ can take one of the three values

$$\begin{aligned}
&U(X_1, \ldots, X_4),\\
&(23)(U)(X_1, \ldots, X_4) = X_1X_3 + X_2X_4,\\
&(24)(U)(X_1, \ldots, X_4) = X_1X_4 + X_2X_3.
\end{aligned}$$

The elements of S_4 that leave U fixed are those of the group H_1 mentioned in §16.2.5, and those that leave $(23)U$ fixed are those of the group $(23)H_1(23) = H_2$. Finally, those that leave $(24)U$ fixed are those of the group $(24)H_1(24) = H_3$.

Let us form the *D_4-resolvent*, the polynomial defined by

$$R(X) = (X - (x_1x_2 + x_3x_4))(X - (x_1x_3 + x_2x_4))(X - (x_1x_4 + x_2x_3)).$$

We now need an elementary result on algebraic integers; this is an extremely important notion in number theory which we have not used up to now. A

algebraic number over $\mathbb{Q}$ is an *algebraic integer* if its minimal polynomial has integral coefficients. We will assume the (true) result that the sum and the product of two algebraic integers are also algebraic integers; this result can be shown using resultants.

PROPOSITION. – $R(X) \in \mathbb{Z}[X]$.

PROOF. –

1) By the result just cited, the roots of R are algebraic integers, so the coefficients of R are also algebraic integers.

2) For every $\sigma \in G$, we have $\sigma(R)(X) = R(X)$; the coefficients of R are invariant under every element of G, so they lie in $\mathbb{Q}$ and are computable using results on symmetric polynomials (see Chapter 3).

3) The only algebraic integers in $\mathbb{Q}$ are the elements of $\mathbb{Z}$, which gives the result. ◊

PROPOSITION. – *Assume that R has only simple roots. Then,*

$\Phi(G) \subset H_1$ if and only if $x_1x_2 + x_3x_4$ is an integral root of R,
$\Phi(G) \subset H_2$ if and only if $x_1x_3 + x_2x_4$ is an integral root of R,
$\Phi(G) \subset H_3$ if and only if $x_1x_4 + x_2x_3$ is an integral root of R.

PROOF. – Suppose that $\Phi(G) \subset H_1$. For every $\sigma \in G$, we have $s = \Phi(\sigma) \in H_1$, so

$$\sigma(x_1x_2 + x_3x_4) = x_1x_2 + x_3x_4.$$

Consequently, $x_1x_2+x_3x_4 \in \mathbb{Q}$. Because $x_1x_2+x_3x_4$ is an algebraic integer, it follows that $x_1x_2 + x_3x_4 \in \mathbb{Z}$.

Suppose that $\Phi(G) \not\subset H_1$. Then there exists σ in G such that $s = \Phi(\sigma) \notin H_1$, so $\sigma(x_1x_2 + x_3x_4)$, which is a conjugate of $x_1x_2 + x_3x_4$, is one of the two other roots of R. Because the roots of R are distinct, we have $\sigma(x_1x_2 + x_3x_4) \neq x_1x_2 + x_3x_4$.

Consequently, $x_1x_2 + x_3x_4 \notin \mathbb{Q}$, so $x_1x_2 + x_3x_4 \notin \mathbb{Z}$. ◊

REMARK. – In the case where R has a multiple root, the preceding criterion is not applicable. This difficulty can be avoided, for instance, by modifying the polynomial without changing its Galois group.

16.2.8 Study of $\Phi(G) \subset \mathbb{Z}/4\mathbb{Z}$

Here, again, we want to determine if $\Phi(G)$ is contained in one of the three subgroups of S_4 isomorphic to $\mathbb{Z}/4\mathbb{Z}$. This study can be done only in the

case where the preceding paragraph gives rise to a positive answer. Assume, therefore, that we have shown that $\Phi(G) \subset H_2$, and let us seek to determine if $\Phi(G) \subset K_2$. Consider the polynomial

$$V(X_1, \ldots, X_4) = X_1X_2^2 + X_2X_3^2 + X_3X_4^2 + X_4X_1^2.$$

If $s \in H_2$, then $s(V)(X_1, \ldots, X_4)$ can take one of the two values

$$\begin{aligned} &V(X_1, \ldots, X_4) \quad \text{or} \\ &(13)(V)(X_1, \ldots, X_4) = X_3X_2^2 + X_2X_1^2 + X_1X_4^2 + X_4X_3^2. \end{aligned}$$

The elements of H_2 that leave V fixed are those of the group K_2.

Let us form the $(\mathbb{Z}/4\mathbb{Z})$-*resolvent*, the polynomial given by

$$R(X) = (X-(x_1x_2^2+x_2x_3^2+x_3x_4^2+x_4x_1^2))(X-(x_3x_2^2+x_2x_1^2+x_1x_4^2+x_4x_3^2)).$$

PROPOSITION. – *Suppose that R has only simple roots. Then $\Phi(G) \subset K_2$ if and only if $y = x_1x_2^2 + x_2x_3^2 + x_3x_4^2 + x_4x_1^2$ is an integral root of R.*

PROOF. – The proof is the same as the proof of the proposition of the preceding section.

If $\Phi(G) \subset K_2$, then for every $\sigma \in G$, we have $s = \Phi(\sigma) \in H_2$, so $\sigma(y) = y$. Consequently, $y \in \mathbb{Q}$. As y is an algebraic integer, it follows that $y \in \mathbb{Z}$.

If $\Phi(G) \not\subset K_2$, there exists σ in G such that $s = \Phi(\sigma) \notin K_2$, so $\sigma(y)$, which is a conjugate of y, is the other root of R. Because the roots of R are distinct, we have $\sigma(y) \neq y$. Consequently, $y \notin \mathbb{Z}$. ◇

REMARK. – We can also study $\Phi(G) \subset K_1$ or $\Phi(G) \subset K_3$ by this method, by renumbering the roots.

16.2.9 An Algorithm for $n = 4$

Let P be a polynomial of degree 4 in $\mathbb{Q}[X]$.

1) We first reduce to the case of a monic polynomial with integral coefficients (see §16.2.1).

2) We check that P is irreducible over $\mathbb{Q}$.

3) We compute good approximations of the roots of P in $\mathbb{C}$.

4) We test to see if $\Phi(G) \subset A_4$ (see §16.2.6).

5) We test to see if $\Phi(G) \subset D_4$ (see §16.2.7).

If the answer is

$$\begin{aligned}
&4 : \text{yes},\ 5 : \text{yes}, && \text{then } G \simeq V;\\
&4 : \text{yes},\ 5 : \text{no}, && \text{then } G \simeq A_4;\\
&4 : \text{no},\ \ 5 : \text{no}, && \text{then } G \simeq S_4;\\
&4 : \text{no},\ \ 5 : \text{yes}, && \text{we do test 6) below.}
\end{aligned}$$

6) We test to see if $\Phi(G) \subset \mathbb{Z}/4\mathbb{Z}$ (see §16.2.8).
If the answer is

$$\begin{aligned}
&6 : \text{yes}, && \text{then } G \simeq \mathbb{Z}/4\mathbb{Z};\\
&6 : \text{no}, && \text{then } G \simeq D_4.
\end{aligned}$$

BIBLIOGRAPHICAL NOTE. – To study recent developments of these methods, see the articles by A. Valibouze and their bibliographies.

Bibliography

The recent books cited here are available in most university libraries. For the older books, it takes a bit of luck to find them, and you may find yourself searching for years, like the scholars of the Middle Ages seeking for rare manuscripts.

Recall that an introduction to Galois theory can be found in every basic algebra book; we have made use of such books in writing this one, for example, N. Bourbaki (chapter V of *Algebra*), the more advanced book *Algebra, volume 2* by MacLane and Birkhoff, Jacobson's *Basic algebra*, and Lang's *Algebra*.

ABEL Niels Henrik (1802–1829). – *Oeuvres complètes* (French, two volumes). Imprimerie de Grondhal & Son, Christiania, 1881.

The two articles on the impossibility of resolving equations of degree 5 and higher are contained in volume 1, pp. 28–33 and 66–94. The second of these articles first appeared in *Journal für die reine und angewandte Mathematik*, founded in 1825 by a friend of Abel named August Leopold Crelle. Many other articles by Abel were published in this journal. For a biography of Abel, see the book by Oystein Ore listed below.

ABHYANKAR Shreeram S. – Fundamental group of the affine line in positive characteristic. In *Geometry and analysis* (Bombay, 1992). Tata Inst. Fund. Res., Bombay, 1995, pp. 1–26.

In this article, the author discusses what he calls *the surprise of the century.* Let P be a polynomial of degree n in $K[X]$, irreducible over K. Choose a root x_1 of P, and set $P_1 = P/X - -x_1$. If P_1 is irreducible

over $K[x_1]$, choose a root x_2 of P_1 and set $P_2 = P_1/X - -x_2$. Iterate this procedure until you obtain a reducible polynomial. Among the results obtained by this method, note the following surprise: if P_1, P_2, P_3, P_4, and P_5 are all irreducible, then $P_6, \ldots, P_{n--3}$ are irreducible as well!

AD DIN AT TUSI SHARAF. – *Œuvres* (French, 2 volumes), R. Rashed, ed. Les Belles Lettres, Paris, 1986.

APMEP. – *Présence d'Évariste Galois.* no. 48, 1982, 57 pages.
This booklet by the French Association of Mathematics Teachers in Public Education reproduces about 15 texts by Galois and also contains texts by R. Taton: "Évariste Galois et ses contemporains", J. Dieudonné: "L'influence de Galois", and A. Dahan–Dalmedico: "Résolubilité des équations par radicaux et premier mémoire d'Évariste Galois".

ARTIN Emil. – *Galois theory.* Dover Publications, Mineola, NY, 1998 (orig. publ. 1942).
Artin is one of the founders of the modern exposition of Galois theory.

ARTIN Michael. – *Algebra.* Prentice–Hall, Englewood Cliffs, NJ, 1991.
A recent and very agreeable book, at the level of juniors and seniors in college, covering various different parts of algebra, Galois theory in particular (pp. 492–584).

BAKER Alan. – *Transcendental number theory.* Cambridge Mathematical Library, Cambridge University Press, Cambridge, U.K., 1990.
The transcendence of e and π is proved in the very first pages of this small book.

BOURGNE Robert, AZRA J.-P. – *Écrits mathmatiques d'Évariste Galois.* Gauthier–Villars & Cie, Paris, 1962, 541 pages.
This book (reedited in 1976) contains every extant work by Galois, down to his smallest computations, and 15 pages of reproductions of his manuscripts. Additional details can be found in the articles written by the authors/editors for the 1983 Abel–Galois conference in Lille.

CARDAN Girolamo. – *Hieronymi Cardani, præstantissimi mathematici, philosophi, ac medici, ARTIS MAGNÆ, sive de regulis algebraicis...* Ioh. Petreium, Nüremberg, 1545.
This book treats the resolution of all of the different cases of the resolution of third-degree equations in detail. An English translation is available (M.I.T. Press, 1968, 267 pages).

CARREGA Jean–Claude. – *Théorie des corps. La règle et le compas.* Hermann, Paris, 1981 (new ed. in 1989), 277 pages.
This is an elementary book that contains a great deal of geometry.

CHILDS Lindsay. – *A concrete introduction to higher algebra.* Springer–Verlag, New York, 1979.

This book contains a presentation of Berlekamp's algorithm.

DALMAS Andr. – *Évariste Galois révolutionnaire et géomètre.* Le nouveau commerce, Paris, 1982 (new ed. of the 1956 orig.), 184 pages, 16 pages of documents.

This book contains an account of Galois' life, some texts by Galois, and some documents, written by a writer who is in general rigorous, although his tentative identification of the "infamous coquette" may be questionable.

DOUADY Adrien, DOUADY Régine. – *Algèbre et théories galoisiennes.* Cedic, Paris, 1979.

The Galois theory can be found on pages 75–117 of volume 2 of this advanced book.

EDWARDS Harold M. – *Galois theory.* Springer–Verlag, New York, 1984.

In this book, the theory is presented according to the methods of those who created it: Lagrange, Gauss, Abel, Galois, and the others.

EULER, Leonhard (1707–1783). – *Complete works.* 29 volumes.

GAAL, Lisl. – *Galois theory with examples.* Chelsea Publ. Co, New York, 1973, 248 pages.

GARLING D.J.H. – *Galois theory.* Cambridge University Press, New York, 1986, 167 pages.

Elementary.

GAUSS Carl Friedrich (1777–1855). – *Recherches arithmétiques* (trad. par A.–C.–M. Poullet–Delisle). Courcier, Paris, 1807.

The original work by Gauss was in Latin, published in 1801. It contains his research on the quadratic reciprocity law and roots of unity, in particular, on the regular polygon with 17 sides.

GIRARD Albert (1595–1632). – *Invention nouvelle en l'algèbre par Albert Girard mathématicien. Tant pour la solution des équations, que pour recognoistre le nombre des solutions qu'elles reçoivent, avec plusieurs choses qui sont nécessaires à la perfection de ceste divine science, suivi de: de la mesure de la superfice* (sic) *des triangles et polygones sphéricques, nouvellement inventée.* Guillaume Iansson Blaeuw, Amsterdam, 1629, 64 pages.

HOUZEL Christian. – Les principaux thèmes dans l'histoire des équations algébriques. In *Actes de l'Université d'été sur l'histoire des mathématiques*, 1984, Commission Inter–IREM Épistémologie.

This article was the basis of Chapter 1 of this book.

HOUZEL Christian. – La résolution des équations algébriques. In *Sciences à l'époque de la Révolution française.* Albert Blanchard, Paris, 1988, pp. 17–37.

This is a very precise study of work on algebraic equations from Euler to Vandermonde, Lagrange, and Ruffini, with a complete bibliography.

IREM de Paris VII. – *M.A.T.H.*, vol. 2, pp. 70–77.

This is a presentation of part of al Khwarizmi's work on second-degree equations.

LACROIX, Sylvestre François (1765–1843). – *Complément des éléments d'algèbre à l'usage de l'École centrale des Quatre Nations.* Bachelier, Paris, 1835.

This sixth edition contains the final note on Galois quoted in Chapter 13.

LAGRANGE Joseph Louis (1736–1813). – Réflexions sur la résolution algébrique des équations. In *Nouveaux mémoires de l'Académie de Berlin*, volumes of 1770 and 1771.

LAGRANGE Joseph Louis. – *Œuvres.* Gauthier–Villars (et fils), Paris, 1867–1892, vol. 3, pp. 205–421.

A reproduction of the 1770–1771 article.

LAGRANGE Joseph Louis. – *De la Résolution des équations numériques de tous les degrés.* Duprat, Paris, an 6, 268 pages.

LAGRANGE Joseph Louis. – *Traité de la résolution des équations numé--riques de tous les degrés avec des notes sur plusieurs points de la théorie des équations algébriques*, 3rd edition. Bachelier, Paris, 1826.

LIDL R., NIEDERREITER H. – *Finite fields.* Cambridge University Press, New York, 1994.

This new edition of a book first published in 1983 contains beautiful chapters on finite fields and code theory.

MATZAT B. H. – *Konstruktive Galoistheorie. Lecture Notes in mathematics*, vol. 1284, Springer–Verlag, New York, 1987.

This book gives a complete, advanced exposition of recent results on the inverse Galois problem introduced in Chapter 16.

MINAČ Jan, REIS Clive. – Trigonometry in finite fields. *Exposition Math.*, 11, 1993.

MUTAFIAN Claude. – *Équations algébriques et théorie de Galois.* Vuibert, Paris, 1980, 264 pages.

A detailed, concrete, tranquil progression containing many examples.

ORE Oystein. – *Abel. Un mathématicien romantique.* Berlin–Paris, 1989.

A biography of the famous, deeply imaginative Norwegian mathematician who was celebrated by Crelle, Legendre, and Jacobi but never obtained a job in his lifetime, either in Norway or in Berlin. He remained too poor to marry the girl who had been his fiancée since 1823, and finally died in her arms on April 5, 1829, at the age of 26.

RIBENBOIM Paulo. – *Algebraic numbers.* Wiley–Interscience, New York, 1972, 300 pages.

ROTMAN Joseph. – *Galois theory.* Springer–Verlag, New York, 1990, 108 pages.

Elementary.

SAMUEL Pierre. – *Théorie algébrique des nombres.* Hermann, Paris, 1967.

This classic textbook is mainly devoted to the study of algebraic integers. It contains the proof of d'Alembert's theorem given as an exercise in Chapter 7 of this text.

SERRE Jean–Pierre. – *Cours d'arithmétique.* Paris, P.U.F., 1977, 2nd edition.

Exists in English.

SERRE Jean–Pierre. – *Topics in Galois Theory.* Jones and Bartlett, Boston, Londres, 1992, 117 pages.

An advanced exposition of recent result on the inverse Galois problem introduced in Chapter 16 of this book.

STAUDUHAR Richard. – The determination of the Galois groups. In *Mathematics of computation*, vol. 27, no. 124, 1973, pp. 981–996.

STEINITZ E. – Algebraische Theorie der Körpern. *Journal de Crelle*, 1910, pp. 167–309.

STEWART Ian. – *Galois theory.* Chapman and Hall, 1973, 226 pages.

The author of this book is well–known for his tales and drawings. His book is extremely attractive and agreeable.

TATON René. – Évariste Galois et ses biographes. In *Colloque Abel–Galois.* Lille, France, 1983, 30 pages.

Nothing appears to have been omitted from this extremely precise article, which is followed by an extensive bibliography.

TIGNOL Jean–Pierre. – *Leçons sur la théorie des équations.* UCL, Louvain la neuve, 1980.

TIGNOL Jean–Pierre. – *Galois' theory of algebraic equations.* Longman Scientific & Technical, 1987, 429 pages.

This book, which is based on the 1980 "Lessons", is very pleasant. It provides a profound explanation of the history of the theory of algebraic equations through the work of Galois.

VANDERMONDE Alexandre Théophile (1735–1796). – *Histoire de l'Acadé- -mie Royale des Sciences de Paris.* Volumes de 1771.

VAN DER WAERDEN Bartel Leendert. – *Modern algebra.* Frederick Ungar Publ. Co, New York, 1949, 2 volumes.

This famous textbook on modern algebra was first edited in German, in the 1930s; the author was strongly influenced by Emmy Noether. The presentation of Galois theory follows Emil Artin's approach.

VAN DER WAERDEN Bartel Leendert. – *A history of algebra.* Springer–Verlag, New York, 1985.

VIÈTE Franois (1540–1603). – *Opera mathematica in unem volumen congesta... opera atque studio Francisci Schooten Leydensis...* Bonaventuræet Abrahami Elzeviriorum, Lugduni Batavorum, 1646.

This book was edited in Latin by F. Van Schooten, 43 years after Viète's death; Viète's original notation was not preserved. A literal translation by Jean Peyroux exists, published by the bookstore A. Blanchard, 1991. Older texts by Viète are extremely rare.

WANTZEL Pierre Laurent (1814–1848). – Recherches sur les moyens de reconnaître si un problème de géométrie peut se résoudre avec la règle et le compas. In *Journal de mathématiques pures et appliquées*, vol. 2, 1837, pp. 366–372.

WEBER Henri. – *Traité d'algèbre supérieure.* Gauthier–Villars, Paris, 1898.

Galois theory of 100 years ago, presented without the use of linear algebra.

YOUSCHKEVITCH Adolf P. – *Les mathématiques arabes (VIIIième – XVième siècles).* Vrin, Paris, 1976.

A very precise and complete book on the subject.

Index

Graduate Texts in Mathematics

(continued from page ii)

125 BERENSTEIN/GAY. Complex Variables: An Introduction.
126 BOREL. Linear Algebraic Groups. 2nd ed.
127 MASSEY. A Basic Course in Algebraic Topology.
128 RAUCH. Partial Differential Equations.
129 FULTON/HARRIS. Representation Theory: A First Course.
Readings in Mathematics
130 DODSON/POSTON. Tensor Geometry.
131 LAM. A First Course in Noncommutative Rings.
132 BEARDON. Iteration of Rational Functions.
133 HARRIS. Algebraic Geometry: A First Course.
134 ROMAN. Coding and Information Theory.
135 ROMAN. Advanced Linear Algebra.
136 ADKINS/WEINTRAUB. Algebra: An Approach via Module Theory.
137 AXLER/BOURDON/RAMEY. Harmonic Function Theory.
138 COHEN. A Course in Computational Algebraic Number Theory.
139 BREDON. Topology and Geometry.
140 AUBIN. Optima and Equilibria. An Introduction to Nonlinear Analysis.
141 BECKER/WEISPFENNING/KREDEL. Gröbner Bases. A Computational Approach to Commutative Algebra.
142 LANG. Real and Functional Analysis. 3rd ed.
143 DOOB. Measure Theory.
144 DENNIS/FARB. Noncommutative Algebra.
145 VICK. Homology Theory. An Introduction to Algebraic Topology. 2nd ed.
146 BRIDGES. Computability: A Mathematical Sketchbook.
147 ROSENBERG. Algebraic K-Theory and Its Applications.
148 ROTMAN. An Introduction to the Theory of Groups. 4th ed.
149 RATCLIFFE. Foundations of Hyperbolic Manifolds.
150 EISENBUD. Commutative Algebra with a View Toward Algebraic Geometry.
151 SILVERMAN. Advanced Topics in the Arithmetic of Elliptic Curves.
152 ZIEGLER. Lectures on Polytopes.
153 FULTON. Algebraic Topology: A First Course.
154 BROWN/PEARCY. An Introduction to Analysis.
155 KASSEL. Quantum Groups.
156 KECHRIS. Classical Descriptive Set Theory.
157 MALLIAVIN. Integration and Probability.
158 ROMAN. Field Theory.
159 CONWAY. Functions of One Complex Variable II.
160 LANG. Differential and Riemannian Manifolds.
161 BORWEIN/ERDÉLYI. Polynomials and Polynomial Inequalities.
162 ALPERIN/BELL. Groups and Representations.
163 DIXON/MORTIMER. Permutation Groups.
164 NATHANSON. Additive Number Theory: The Classical Bases.
165 NATHANSON. Additive Number Theory: Inverse Problems and the Geometry of Sumsets.
166 SHARPE. Differential Geometry: Cartan's Generalization of Klein's Erlangen Program.
167 MORANDI. Field and Galois Theory.
168 EWALD. Combinatorial Convexity and Algebraic Geometry.
169 BHATIA. Matrix Analysis.
170 BREDON. Sheaf Theory. 2nd ed.
171 PETERSEN. Riemannian Geometry.
172 REMMERT. Classical Topics in Complex Function Theory.
173 DIESTEL. Graph Theory. 2nd ed.
174 BRIDGES. Foundations of Real and Abstract Analysis.
175 LICKORISH. An Introduction to Knot Theory.
176 LEE. Riemannian Manifolds.
177 NEWMAN. Analytic Number Theory.
178 CLARKE/LEDYAEV/STERN/WOLENSKI. Nonsmooth Analysis and Control Theory.
179 DOUGLAS. Banach Algebra Techniques in Operator Theory. 2nd ed.
180 SRIVASTAVA. A Course on Borel Sets.
181 KRESS. Numerical Analysis.
182 WALTER. Ordinary Differential Equations.
183 MEGGINSON. An Introduction to Banach Space Theory.
184 BOLLOBAS. Modern Graph Theory.
185 COX/LITTLE/O'SHEA. Using Algebraic Geometry.
186 RAMAKRISHNAN/VALENZA. Fourier Analysis on Number Fields.
187 HARRIS/MORRISON. Moduli of Curves.
188 GOLDBLATT. Lectures on the Hyperreals: An Introduction to Nonstandard Analysis.

189 LAM. Lectures on Modules and Rings.
190 ESMONDE/MURTY. Problems in Algebraic Number Theory.
191 LANG. Fundamentals of Differential Geometry.
192 HIRSCH/LACOMBE. Elements of Functional Analysis.
193 COHEN. Advanced Topics in Computational Number Theory.
194 ENGEL/NAGEL. One-Parameter Semigroups for Linear Evolution Equations.
195 NATHANSON. Elementary Methods in Number Theory.
196 OSBORNE. Basic Homological Algebra.
197 EISENBUD/HARRIS. The Geometry of Schemes.
198 ROBERT. A Course in p-adic Analysis.
199 HEDENMALM/KORENBLUM/ZHU. Theory of Bergman Spaces.
200 BAO/CHERN/SHEN. An Introduction to Riemann–Finsler Geometry.
201 HINDRY/SILVERMAN. Diophantine Geometry: An Introduction.
202 LEE. Introduction to Topological Manifolds.
203 SAGAN. The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Function. 2nd ed.
204 ESCOFIER. Galois Theory.
205 FÉLIX/HALPERIN/THOMAS. Rational Homotopy Theory.